Report of the National Task Force on the Commercial Sale of Criminal Justice Record Information

SEARCH
The National Consortium for Justice Information and Statistics

This report was prepared by SEARCH, The National Consortium for Justice Information and Statistics, Francis X. Aumand III, Chairman, and Ronald P. Hawley, Executive Director.

This report was produced as a product of a project funded by the Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice, under Cooperative Agreement No. 96-BJ-CX-K010, awarded to SEARCH Group, Incorporated, 7311 Greenhaven Drive, Suite 145, Sacramento, California 95831. Contents of this document do not necessarily reflect the views or policies of the Bureau of Justice Statistics or the U.S. Department of Justice.

Copyright © SEARCH Group, Incorporated, dba SEARCH, The National Consortium for Justice Information and Statistics, 2005.

Contents

Executive summary

Today, background checking—for employment purposes, for eligibility to serve as a volunteer, for tenant screening, and for so many other purposes—has become a necessary, even if not always a welcome, rite of passage for almost every adult American. Like a medical record, a bank record, or a credit record, a background check record is increasingly a part of every American's information footprint.

But, with tens of millions of background checks being conducted annually and with almost all of these checks requiring a search of criminal history record databases, how will all of these checks get done? More and more, the answer is the commercial background screening industry.

This report is the first-ever comprehensive look at the role that commercial background screening companies play in the collection, maintenance, sale, and dissemination of criminal history record information for employment screening and other important risk management purposes.

Part I of this report looks at the burgeoning commercial background screening industry. The report examines the type of information, including the type of criminal history information, that is collected, compiled, maintained, and sold by commercial screeners. What companies comprise the background screening industry; how big are they; are they publicly traded; and how fast are they really growing are all questions addressed, often for the very first time, in this report.

This report also examines the very different business models that the commercial screening industry employs. Some screeners engage in a customized search for criminal history record information each and every time they receive a background screening assignment. These types of companies customarily send "runners" to appropriate courthouses and other repositories that are likely sources of relevant information.

Other screeners purchase automated criminal history records from courts and/or various law enforcement agencies "in bulk." Still other background screening companies maintain their own, surrogate national criminal history record files. Indeed, today, several companies compile and manage criminal history databases with well in excess of 100 million criminal history records.

Part II of this report examines the relevant law. Much of this law addresses the circumstances under which commercial background screeners can obtain access to criminal history record information held by the courts or by executive branch agencies. The law, most of which is State statutory law and implementing regulations but some of which is Federal law, pivots partly on the subject matter of the criminal history information—conviction information, for example, is customarily more available than arrest-only information. The law also pivots on the intended use of the criminal history record information, with employers and their agents and contractors (commercial screeners) increasingly armed with State and Federal authorization to obtain criminal history record information for particular types of employment.

However, by far the most salient legal consideration affecting commercial vendor access is not content or use of the criminal history record, but rather, the source of the criminal history record. Criminal history data maintained by the courts, for the most part, continue to be publicly available. The very same information maintained by State central repositories or State identification bureaus or maintained at the Federal level by the Federal Bureau of Investigation (FBI) is less apt to be available. Even this traditional dichotomy, however, is changing with new background statutes giving employers, volunteer organizations, and landlords, as well as their commercial vendor surrogates, a legal basis for access.

This report's legal analysis also focuses on the Federal Fair Credit Reporting Act (FCRA). This comprehensive law applies to the communication of most types of personal information, including criminal history information, by commercial vendors to authorized users, including employers and landlords. The FCRA is, perhaps, the least understood

and most underrated privacy protection statute.

The report identifies and analyzes, in some detail, the FCRA's numerous privacy protections, including a requirement that applicants and employees who are subject to a commercial vendor background check receive notice and provide consent. In the event that criminal history information is found and used, the FCRA also requires that employees be given an opportunity to review and correct or contest the accuracy of criminal history information. Furthermore, the FCRA prohibits commercial vendors and employers and other authorized users from redisseminating or reusing a criminal history record report for other purposes.

Part III of this report looks at the compelling public policy issues that arise from the commercial sale of criminal history record information. In order to provide texture and depth to this analysis, SEARCH convened a Task Force comprised of experts and stakeholders. The Task Force included representatives of State central repositories and State identification bureaus; representatives of the FBI; representatives of the courts; leaders of the commercial screening industry; representatives of employers and also of volunteer groups; privacy advocates; and academic experts and researchers.

The Task Force provided invaluable input about the size and composition of the screening industry. The Task Force members also provided nuance and insight about the way in which relevant law is implemented and enforced.

Most importantly, however, the Task Force analyzed and debated the key public policy issues that arise from the growing importance of the screening industry. The Task Force reached consensus and made recommendations on several of these public policy issues:

- The Task Force recommended that the important and comprehensive protections in the Federal FCRA apply, not only when a commercial vendor communicates criminal history information to an employer or other authorized users, but also when employers and others go directly to the courts or executive branch repositories to obtain criminal history record information for employment and other authorized purposes.
- The Task Force called for guidance to be developed and provided to the users of criminal history information regarding the meaning and relevancy of criminal history information. Part of this "criminal history literacy" recommendation is aimed at assisting users in understanding how to read and interpret a rap sheet. Another part of this literacy recommendation is intended to "connect the dots" between the existence of a criminal history record and the extent to which, and the way in which, that record is relevant to predictions about performance on the job; in volunteer positions; as a tenant; or in other situations where background checking is being used.
- The Task Force also recommended that the commercial screening industry develop biometric identification protocols. At present, the commercial screening industry relies primarily upon name, plus other identifiers, to make an identification of an individual. The industry has greatly improved the reliability of name-based identification tools. Nevertheless, the Task Force called for the industry to continue its efforts to incorporate a biometric—primarily a fingerprint—into its identification verification methodologies.
- The Task Force cautioned against the exclusion of identifiers from public records. The Task Force noted that, increasingly, changes in law restrict the inclusion of Social Security numbers and other identifiers in public records, including criminal history records. The Task Force believes that this trend inevitably will increase the risk that the wrong file will be associated with the wrong person. Moreover, this trend, if it persists, poses a threat not only to the quality of background checking, but also to efforts to prevent identification fraud.

For other key public policy issues, the Task Force did not provide recommendations, but its insight and analyses are captured in Part III of this report. These issues are:

- A discussion of whether changes in law should be made to the FCRA.

- An analysis of the impact of the availability of commercial vendor criminal history record information on offenders who are released from incarceration and the related "reintegration" crisis.

- The quality, completeness, accuracy, and timeliness of criminal history information included in commercial vendor background checks.

- The merits and the threats arising from data linkage, data mining, and profiling and, in particular, the pivotal role played by criminal history information and commercial vendors in this process.

The Task Force believes that this report will provide invaluable information about the sale of criminal history information by commercial vendors for employment and other background check purposes. The Task Force also hopes that its analyses and recommendations will make a significant contribution to this ongoing and very important public policy debate.

Introduction

A. Background checks post-September 11

In the aftermath of the terrorist attacks of September 11, 2001, the Nation has seen an explosion in criminal background checks. Legislation passed by Congress after the September 11 attacks requires new or expanded background checks in an array of areas, such as airline and airport personnel, port workers, and truck drivers who transport hazardous materials. Federal agencies have also recommended, rather than required, background checks as well. The Food and Drug Administration (FDA), for example, has issued nonbinding "good practice" guidelines recommending that food establishment operators conduct criminal background checks on all employees.[1] Even in the absence of government requirements or encouragement, many in the private sector also have expanded the extent to which they conduct criminal background checks on their employees, business partners, and customers.

This growth, which many expect will continue or increase in the months and years ahead, raises a host of issues with respect to how best to conduct the required background checks in the most prompt, efficient, and privacy-sensitive manner possible. An important component of these background checks will be criminal justice record information, which broadly includes information arising from an individual's arrest, conviction, or other interaction with the criminal justice system.

The criminal justice record information included in background checks comes mainly from four sources:

1. law enforcement, including the Federal Bureau of Investigation (FBI) and State central criminal history repositories
2. the courts
3. corrections agencies
4. commercial vendors that collect criminal justice record information from the courts or through whatever access State laws provide to law enforcement or corrections records.

Discrete laws and regulations govern each of these sources. This frequently means that different information is available to different types of users, depending upon the source from which the information is obtained.

The fourth source, commercial vendors, is essentially an alternative means of distributing criminal justice record information that is already available from government sources. The role of commercial vendors generally has been described by a public record advocacy organization as "collect[ing] records from disparate sources and mak[ing] them available conveniently, reliably, and at low cost. These commercial information providers *both* enhance access, with all of its benefits, *and* greatly reduce the burden on government clerks by filling many requests for records that would otherwise consume public resources."[2]

Given the increasing demand for criminal background checks—and the pressure that such demand is expected to place on courts, the FBI, and State criminal history repositories—the Bureau of Justice Statistics (BJS), U.S. Department of Justice, and SEARCH, The National Consortium for Justice Information and Statistics, established a National Task Force on the Commercial Sale of Criminal Justice Record Information to examine the role played by commercial vendors in the sale of criminal justice record information.[3]

[1] The FDA defines operators of a food establishment to include firms that produce, process, store, repack, relabel, distribute, or transport food or food ingredients. "Guidance for Industry: Food Producers, Processors, and Transporters: Food Security Preventive Measures Guidance," U.S. Department of Health and Human Services, U.S. Food and Drug Administration, Center for Food Safety and Applied Nutrition (March 21, 2003) (recommending that operators have "a criminal background check performed by local law enforcement or by a contract service provider"). Hereafter, FDA Guidance. A version of the guidance issued on Jan. 9, 2002, also recommended checking the "Federal Bureau of Investigation Watchlist."

[2] *Public Benefits from Open Public Records*, CSPRA Public Records White Paper series (Arlington, Va.: Coalition for Sensible Public Record Access, undated) at p. 3, available at <www.cspra.org> (emphasis in original).

[3] The project was funded by and operated under the auspices of BJS in the Office of Justice Programs, U.S. Department of Justice. Since its inception, BJS has taken a leadership role in the improvement of criminal history record information and the development of appropriate policies for handling this information (*see* <www.ojp.usdoj.gov/bjs/>). SEARCH, The National Consortium for Justice Information and Statistics, is a State criminal justice support

B. Role of the National Task Force

The National Task Force on the Commercial Sale of Criminal Justice Record Information (hereafter, Task Force) consisted of criminal history record managers, commercial vendors of criminal justice record information, court and law enforcement officials, users of background checks, and policy experts. The observations in this report reflect the Task Force's consensus views but do not necessarily reflect the views of any particular Task Force member or of his or her institutional affiliations.[4] The Task Force held a series of multiple-day meetings, including meetings in New York City on March 12–13, 2002, and April 29–30, 2003, and in Chicago on December 5–6, 2002. The Task Force focused its attention on three areas:

1. the structure of the commercial information industry
2. laws, regulations, policies, and practices that impact commercial vendors and end-users of criminal justice information
3. the broader public policy issues associated with criminal background checks.

1. Structure of the commercial information industry

The first focus of the Task Force was to explore ways to ensure that background checks involving criminal justice information can be conducted promptly, efficiently, and completely, while recognizing and protecting the rights of the individuals being checked.

The Task Force examined the structure of the commercial information industry, focusing primarily on the segment of the industry that uses criminal justice record information for background check purposes. The Task Force found that the sale of criminal justice record information by responsible commercial vendors provides societal benefits, which include facilitating economic efficiency and alleviating demand for criminal justice record information that otherwise falls entirely to courts and government agencies for processing.[5] The Task Force also found that commercial vendors can create benefits for end-users of their reports that courts and government agencies are not always able to provide. These benefits range from faster response times, to tailored information products, to information from multiple information sources pertaining to criminal justice record information, as well as other types of information.

The Task Force also considered the implications for privacy and other interests of the individuals who are the subject of criminal background checks being conducted by commercial vendors. The Task Force considered, for example, the accuracy implications of the standard practice of commercial vendors to use name and other descriptors, such as Social Security number, date of birth, and address (commonly referred to as "name-plus-identifier checks"), rather than fingerprints as the basis of associating information with individuals. The Task Force also considered the rights of correction available to individuals and other protections that are in place to safeguard against adverse employment or other actions on the basis of criminal justice record information being incorrectly associated with an individual (that is, "false positives"). Authenticating the identity of individuals is taking on increased importance, with new commercial products and government proposals intended to verify that the individual is who he or she claims to be. This is an interest separate from, but often interrelated with, an interest in determining whether there is criminal justice or other information associated with the individual.

organization comprised of one governor's appointee from each State, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. For more than 35 years, SEARCH has promoted the effective and appropriate use of information, identification, and communications technology for State and local criminal justice agencies (*see* <www.search.org>). For the same period of time, SEARCH has been vitally concerned with the privacy and public access implications of the automation and use of personally identifiable criminal justice record information.

[4] A list of Task Force members is included as the Appendix.

[5] Commercial vendors still must interact with government agencies to compile the information necessary for their background checks. However, the net burden on government agencies is still likely to be reduced because, in some cases, vendors are able to purchase criminal justice record information in bulk to fulfill multiple end-user requests for information, thereby minimizing the workload of government agencies. Even where this is not the case, commercial vendors generally can be expected to be more knowledgeable about the agencies involved and the information being sought than is the case with the average employer or other party requesting a background check.

The Task Force also focused on the relationship between commercial vendors and criminal justice record information sources, such as the courts, law enforcement, State repositories, and corrections agencies.[6] The Task Force examined the diverse means by which, and the sources from which, commercial vendors obtain criminal justice record information, including through the use of court "runners," electronic interfaces with government agencies, and bulk purchases of criminal justice record information from courts or corrections departments. Depending on the information source, the Task Force found that the ability of a particular court, repository, or corrections agency to provide data to commercial vendors was subject to legal restrictions. Such restrictions could prohibit the ability of commercial vendors to obtain criminal justice record information, restrict the manner in which information is provided, or dictate the cost (and sometimes cost effectiveness) of obtaining information from a particular court or agency.

[6]The outsourcing of government functions to private-sector entities and the use of private-sector contractors by courts or government agencies to assist them in the management of criminal justice record information is beyond the scope of this report. Such initiatives are referenced herein only to the extent that they bear on the commercial sale of criminal justice information.

2. Laws, regulations, policies, and practices that impact commercial vendors and end-users of criminal justice information

Second, the Task Force examined Federal and State law, and related regulations, policies, and practices, that have a significant impact on the manner in which commercial vendors and end-users obtain and maintain criminal justice information; the ability of end-users to use that information for employment and other purposes; and the safeguards that must be employed to protect the privacy of individuals to whom the information pertains. With some overlap, these laws, regulations, policies, and practices fall into four broad categories:

1. those that promote, restrict, or otherwise regulate access to criminal justice record information held by governmental sources
2. those that primarily regulate the practices of commercial vendors, such as the Fair Credit Reporting Act
3. those that regulate the information that end-users, particularly employers and landlords, can use to make employment and housing decisions
4. negligence doctrines that promote efforts by employers and landlords to obtain criminal justice record information.

3. Broader public policy issues associated with criminal background checks

Third, the Task Force considered broader public policy issues associated with criminal background checks, identifying areas where changes may be necessary to enhance the ability of both government and commercial vendors to provide information for background check purposes in a timely, complete, and accurate manner. The Task Force kept in mind the need to balance public safety interests and the privacy and civil liberties interests of individual record subjects, as well as other considerations such as reintegrating criminal offenders into society. Public policy issues examined include:

- **Regulation.** Should the information practices of commercial vendors, the courts, State repositories, and corrections departments all be subjected to the same rules?
- **Privacy.** Should the Fair Credit Reporting Act be amended to impose obligations on all end-users of criminal justice record information? Should the Act be amended to reach all commercial criminal justice record information products?

- **Relevancy.** Are there relevancy considerations in the collection, use, and dissemination of criminal justice record information? If so, who determines what is relevant? Is criminal justice record information relevant to anti-terrorism efforts? Should public policy pivot on whether the information in question is arrest information or conviction information?
- **Reintegration.** Each year, approximately 650,000 offenders are released from incarceration. If commercial vendors retain criminal justice record information indefinitely (and make this information available indefinitely), does this frustrate efforts to reintegrate these offenders into society?
- **Biometrics.** Should commercial vendors be permitted/encouraged/required to use a biometric (presumably, a fingerprint) when identifying individuals who are subject to criminal background checks and when matching a criminal justice record with an individual?
- **Data Quality.** If (and this is very much a question) commercial vendor criminal justice record checks suffer from incompleteness or inaccuracy or staleness, what, if anything, should be done about this from a public policy standpoint?
- **Profiling.** When commercial vendors combine criminal justice data with other personal data to create "profiles," what are the public safety and risk management benefits, and what are the privacy threats? Should public policy be developed to address these issues?

Part I. The commercial criminal justice record information industry

Part I focuses on the structure of the segment of the commercial information industry that deals in criminal justice information. The following discussion is based on information furnished by commercial vendors who participated on the Task Force, as well as independent research. The industry description should be viewed as a "snapshot" of the state of the industry at the time this report was prepared. It should be noted, however, that this industry is rapidly evolving as a result of such factors as advances in technology, the development of new products, growing demand, increased efficiencies, and industry consolidation.

It is also important to note that while the focus of this report is commercial vendors dealing in criminal justice information, these vendors often offer their clients additional information products and services—such as employment history verification, identity authentication, address verification, credit reports, and drug-screening services.

A. Types of personal information sold by commercial vendors

1. Criminal justice record information

The primary focus of this report is on commercial vendors that sell criminal justice record information. For purposes of this report, criminal justice record information means, in large part, traditional criminal history record information pertaining to the arrest (or notice to appear in lieu of arrest); detention; indictment or other formal criminal charge (and any conviction, acquittal, or other disposition arising therefrom); sentencing; correctional supervision; or release of an identifiable individual.[7]

Criminal justice record information also includes other information that originates with courts and government agencies, including sex offender registry information; wanted person information; and protective order information.[8] For purposes of this report, criminal justice record information *does not* include investigative and intelligence information, although it is the sense of the Task Force that commercial vendors would be interested in obtaining nonpublic[9] Terrorist Watch List information if it were available.[10]

Domestic criminal justice record information continues to be the primary source of most traditional background checks. However, particularly in the post-September 11 environment, commercial vendors are increasingly interested in foreign criminal justice record information. Some firms specialize in foreign background investigations.

Criminal justice record information, for the purposes of this report, includes only information pertaining to an identified person that is used for some purpose re-

---

[7] *See* 28 C.F.R. § 20.23(b).

[8] The line between criminal and civil justice information is not necessarily as clear as it once may have been. One Task Force member illustrated this point by noting that in her State, child-support writs, which originate in civil courts, can result in criminal arrest in the event that an individual does not satisfy child-support obligations.

[9] The FBI divides the Terrorist Watch List (TWL) into three categories, only one of which, the Most Wanted Terrorist List, is publicly available. According to the FBI, the TWL contains the following components: "The first category will include the names of individuals for whom formal charges or indictments have been issued (e.g., …individuals on the Most Wanted Terrorist list). The second category will include the names of individuals of investigative interest to the FBI. The third category of the TWL will include the names of individuals provided by the Intelligence Community and cooperating foreign governments." Statement for the Record of Robert J. Jordan, FBI, on Information Sharing Initiatives before the U.S. Senate Committee on the Judiciary Subcommittee on Administrative Oversight and the Courts, Apr. 17, 2002.

[10] It is the sense of the Task Force that commercial vendors do not currently have access to nonpublic portions of the TWL, except to the extent that such access is necessary to provide an information product or service to the government. *See,* e.g., EagleCheck, Ltd., "EagleCheck Receives TSA Approval for Field Trials at Cleveland Hopkins International and Akron-Canton Regional Airports," Press Release (Jan. 23, 2003) available at <www.eaglecheck.com/News/News.htm>. ("At full implementation, EagleCheck can reference the most up-to-date intelligence sources, such as the National Crime Information Center and the Terrorist Watch List, to determine whether potential passengers are known threats.") The Task Force is unaware of nonpublic TWL information being incorporated into background checks provided to potential employers or others.

lating specifically to that person. The use of criminal justice record information for statistical analysis or research purposes is beyond the scope of this report.

2. Other information

It is important to note that criminal justice information is only one facet of a much broader personal-information industry. Commercial vendors customarily deal in three broad categories of information about individuals:[11] public record information, publicly available information, and information from nonpublic sources.

Public record information is derived from public records maintained by the government.[12] Public records are created as a result of virtually every interaction with government. Public records containing personal information include: bankruptcy records; civil court records; birth and death records; licensing records; marriage and divorce records; real property records; tax lien records; voter registration records; motor vehicle records; records pertaining to other modes of transportation, such as boats and airplanes; corporate filings; Uniform Commercial Code filings; Security and Exchange Commission filings; the Office of Foreign Asset Control "blocked person list"[13]; and, of course, criminal justice records.

Although criminal justice record information is the primary focus of this report, it is important to note that many commercial information vendors place their principal focus on other types of public records. Dolan Information, for example, is a leading provider of public records pertaining to bankruptcies, civil judgments, State and Federal tax liens, and eviction notices.[14] Dolan offers access to more than 100 million records in formats ranging from batch processes to online searches.[15] Online searches are offered for bankruptcies nationwide and for public records in 35 States.[16]

Publicly available information is derived from a nonpublic records source that is widely available. Classic examples of publicly available information include telephone books, newspapers, and other periodicals. Publicly available information also includes specialty publications, such as alumni and professional directories.

An example of an information product based on publicly available information is Acxiom's Infobase Telephone Directories product, a database that provides users with access to more than 123 million telephone and address listings throughout the United States and 16 million Canadian listings.[17] The file harvests data from more than 5,000 directories.[18]

Nonpublic information is derived from sources other than public records or publicly available information. Such information may include, but is far from limited to, a consumer's credit history reported to a consumer reporting agency by a merchant or financial services organization; medical information; survey and other self-reported information by an individual; information provided

[11]Of course, there is also a market for non-personally identifiable information, such as statistical and aggregate information. A discussion of the policy issues arising from the use of these types of information products is beyond the scope of this report.

[12]What constitutes a "public record" is a matter of some debate, with some arguing that all government records are public records and should be available to the public because tax dollars pay for their creation and maintenance. This view is not reflective of current law, however, which restricts the availability of some government records on a variety of grounds ranging from national security to privacy. Examples in the latter regard include census data on individual households (not aggregate census data), tax returns, and adoption records. The treatment of public records in this report focuses primarily on records that include personally identifiable information and which are currently available to the public.

[13]Executive Order 13224, issued by President Bush on Sept. 23, 2001, prohibits all U.S. persons and entities from conducting financial transactions (including wages and insurance benefits) with persons or entities identified as having terrorist ties. The Treasury Department's Office of Foreign Asset Control maintains and publishes a list of such persons. Some commercial vendors have integrated this list into their background screening products.

[14]Dolan Information, "About Us," available at <www.dolaninformation.com/about.cfm> (visited Jan. 20, 2004). Dolan Information was purchased by LexisNexis, a member of Reed Elsevier Group plc, in August 2003. Ibid.

[15] Dolan Information, "Products," available at <www.dolaninformation.com/products.cfm> (visited Jan. 20, 2004).

[16]Dolan Information, "Banko Online," available at <www.dolaninformation.com/bankoonline.cfm> (visited Jan. 20, 2004).

[17]Acxiom Corp., "InfoBase® Telephone Directories," available at <www.acxiom.com/default.aspx?ID=1763&Country_Code=USA> (visited Jan. 20, 2004).

[18]Ibid.

by consumers on product warranty cards; and insurance claims data.

Perhaps the most prominent examples of companies providing nonpublic information are the Nation's three national credit-reporting systems: Equifax, Experian, and TransUnion. Consumer reports prepared by these systems may include public record information, such as tax liens or bankruptcy information. The bulk of the data, however, pertain to the existence and payment status of a consumer's credit cards, mortgages, auto loans, student loans, etc. It is estimated that each of the three major credit-reporting systems maintain approximately 190 million consumer credit files and that 2 billion pieces of data are incorporated into these consumer credit files each month.[19] It is also estimated that approximately 1 billion consumer credit reports are issued in the United States every year.[20] Equifax, the largest of the national credit-reporting systems and an S&P 500 company, for example, has more than $1.1 billion in annual revenues and 4,800 employees in 12 countries.[21] During 2001, Equifax's core consumer reporting business produced 357.8 million consumer credit reports.[22] Just 10 years earlier, in 1991, Equifax produced only 103.2 million consumer credit reports.[23]

B. Industry size and scope

The portion of the commercial information industry that provides criminal justice information products is difficult to quantify. In addition to a few large industry players, there are hundreds, perhaps even thousands, of regional and local companies. Given the number of vendors and the variety of business models they employ, the Task Force was unable to quantify the overall number of commercial vendors, the overall number of criminal background checks conducted for noncriminal justice purposes in the United States in a given year, or the overall revenues of this sector of the information industry.

Since comprehensive, industry-wide data are not available, this report instead identifies some of the largest and most innovative players in the criminal justice information segment of the information industry (as well as some niche players) and uses their products as a means to illustrate the types of products that are available. Subsequent sections of this report examine the types of business models that commercial vendors employ (some focus on the compilation of information, which is done in several ways; some sell criminal justice information to end-users; and some both compile *and* sell criminal justice information). This report also provides examples of how much commercial vendors charge for their products and the types of factors that can affect pricing and the industry's customer base.

1. Key industry members

The company with one of the largest commercial criminal justice record information businesses is ChoicePoint, Inc., based in Alpharetta, Ga. ChoicePoint, which is publicly traded on the New York Stock Exchange, has approximately 3,500 employees.[24] ChoicePoint reported nearly $792 million in revenue for 2002.[25] Almost $309 million of this income came from the company's Business and Government Services Division, which includes its employee and tenant screening businesses and its other public record businesses.[26] Over the past several years, ChoicePoint has purchased dozens of other information companies, including at least 11 involved in the employee screening process.[27] ChoicePoint reported that it conducted approximately 3.3 million background investigations during 2002, the vast majority of which included a criminal justice information component.

US Investigations Services (USIS), which was the Office of Federal Investigations before it was privatized in 1996, has more than 5,600 employees operating from 185 locations.[28] USIS reports

[19]Consumer Data Industry Association, "About CDIA," available at <www.cdiaonline.org/about.cfm> (visited Jan. 20, 2004).

[20]Ibid.

[21]Equifax, "About Equifax," available at <www.equifax.com/corp/aboutefx/main.shtml> (visited Jan. 20, 2004).

[22]*2001 Annual Report* (Atlanta: Equifax, Inc., undated) at p. 4.

[23]Ibid.

[24]ChoicePoint, Inc. "Overview," available at <www.choicepoint.com/about/overview.html> (visited Jan. 20, 2004).

[25]*2002 Annual Report* (Alpharetta, Ga.: ChoicePoint, Inc., 2003) at p. 18.

[26]Ibid.

[27]Leslie Walker, "Police Records for Anyone's Viewing Pleasure," *Washington Post* (May 23, 2002) at p. E01. Hereafter, Walker article.

[28]USIS, "Company Profile," available at <www.usis.com/companyprofile.htm> (visited Jan. 12, 2004).

having completed more than 2.4 million investigations each year for its government and commercial clients.[29] USIS has expanded from its traditional government investigation business, in part through acquisitions. In 2002, for example, USIS acquired DAC Services, a firm that specialized in employment screening for the transportation industry.[30] The transportation unit, now named USIS Transportation Services, reports having more than 300 employees and a network of more than 4,000 court runners.[31] USIS Transportation Services reports having approximately 30,000 clients nationwide and processing "in excess of 14 million consumer reports annually."[32]

Other large commercial vendors are also enhancing their criminal background check capabilities. In August 2002, for example, Acxiom, which is based in Little Rock, Ark., announced the acquisition of TransUnion's employment screening unit. The new Acxiom Information Security Services unit, located in Cleveland, has about 140 employees and 1,800 customers nationwide.[33] The company offers a range of products, including "verification of Social Security numbers, criminal record search, reference verification, education verification, and other methods to assess an applicant's character, credentials, and ability to do the job."[34]

LexisNexis, headquartered in Dayton, Ohio, has more than 12,000 employees worldwide and is a member of Reed Elsevier Group plc.[35] LexisNexis offers a range of information products, including searchable access to 4 billion documents obtained from thousands of sources.[36] In June 2002, Lexis announced plans to bolster its criminal justice information offerings through an alliance with National Background Data, Inc.[37]

First Advantage Corporation, created in 2003 as a result of the merger of First American Registry and US Search.com Inc., which has prominently advertised its services on television, is publicly traded on the NASDAQ exchange and has approximately 1,200 employees.[38] The components of the new company had revenues of approximately $160 million in 2002 from a variety of products, including employment background screening; resident screening services; consumer location services; substance abuse management and testing services; and driving records.[39]

National Background Data (NBD), founded in 2000, is a privately held company that specializes in criminal justice information.[40] NBD may have the Nation's "largest privately held criminal records database of its kind."[41] NBD does not provide criminal justice information directly to end-users. Instead, the company provides the data to business partners who, in turn, provide the information to the end-user.[42] As of May 2003, NBD had 17 employees.[43]

Rapsheets.com, a subsidiary of The Daily News Publishing Company of Memphis, bills itself as "the most comprehensive site on the Internet in delivering instant results of criminal records searches" with more than 160 million records.[44] The company

[29]Ibid.

[30]USIS, "USIS Transportation Services Overview," available at <www.usis.com/commercialservices/transportation/companyoverview.htm> (visited Jan. 9, 2004). Hereafter, USIS Transportation Overview.

[31]USIS, "Frequently Asked Questions," available at <www.usis.com/commercialservices/transportation/faq.htm> (visited Jan. 9, 2004).

[32]USIS Transportation Overview, *supra* note 30.

[33]Acxiom Corp., "Acxiom® Expands Its Customer Solutions by Offering Employment Security Screening Services," Press Release (Aug. 12, 2002) available at <www.acxiom.com/default.aspx?ID=1996> (visited June 28, 2004).

[34]Ibid.

[35]National Background Data, "LexisNexis, National Background Data Announce Strategic Alliance," Press Release (July 11, 2002) available at <www.nationalbackgrounddata.com/pdf/nbd_lexisnexis.pdf> (visited Apr. 2, 2004).

[36]Ibid.

[37]Ibid.

[38]First Advantage Corp., "About Us," available at <http://fadv.com/about_us/about_us.html> (visited Jan. 20, 2004).

[39]The First American Corp., "The First American Corporation to Merge Screening Information Business with US SEARCH.COM, Inc.," Press Release (Dec. 16, 2002) available at <www.hirecheck.com/MeetHireCheck/InTheNews/USSearch.asp> (visited June 28, 2004).

[40]*See* <www.nationalbackgrounddata.com>.

[41]National Background Data, "About NBD," available at <www.nationalbackgrounddata.com/com_about.cfm> (visited June 28, 2004).

[42]Ibid.

[43]National Background Data, submission of information to the Task Force (May 23, 2003).

[44]Rapsheets.com, "About Rapsheets Criminal Records," available at <www.rapsheets.com/about.aspx>

began compiling criminal justice record information databases in 1997.[45] Rapsheets.com sells information directly to end-users over the Internet as well as to resellers. By May 2002, the company reportedly had nine employees.[46]

2. Number of records

One method of measuring the industry as a whole, as well as that portion dealing with criminal justice information, is by measuring the number of records.

ChoicePoint reports that it has 17 billion public records. This includes its National Criminal File, which includes more than 90 million criminal records.[47] Other companies report having more criminal justice records than ChoicePoint. NBD's *National Background Directory*, for example, provided, as of spring 2003, real-time access to more than 126 million offense records covering 38 States.[48] Rapsheets.com, which bills itself as "the most comprehensive site on the Internet in delivering instant results of criminal records searches," advertises on its Web site as having more than 160 million records.[49]

These industry figures, of course, do not necessarily mean that these companies hold criminal justice information about 90 or 160 million unique individuals. Because the companies count by record (rather than person), there is considerable potential for overlap. One individual may be the subject of multiple records, due to a conviction on multiple charges, multiple convictions in one jurisdiction, or convictions in multiple jurisdictions. In addition, the same incident may be reflected in multiple sources. If the vendor obtains information both from a State court and a State department of corrections, for example, an individual convicted of an offense may show up once in the court's records and again in a separate record authored by the department of corrections.

C. Commercial vendor business models

Not surprisingly, commercial vendors take a variety of approaches to the packaging and sale of criminal justice record information. These approaches include:

- bulk purchases of criminal justice record information, which is used to create a database for resale of the information as requested
- "gateway purchases," whereby end-users purchase records from a court or criminal justice agency through a database interface facilitated by the vendor
- "traditional" or "one-off" purchases, whereby vendors purchase particular records necessary for the preparation of a report about a specific individual.

1. Compilation of reports

a. "Runners"

The traditional method used by commercial vendors to conduct a criminal background check, once a report is ordered, is to send personnel (sometimes called "runners") to the courts (and sometimes to police departments) in the jurisdictions where the report subject lives or has lived (and sometimes adjoining counties). An inquiry might also be sent to a State criminal history repository, if access to the repository's records is allowed by law. Once the information is received, a report is prepared on the basis of that information and sent to the end-user. Preparation of these reports can be labor-intensive and may take days or sometimes weeks to produce.

Given that a nationwide network of runners would be needed to cover all of the Nation's nearly 3,500 counties, maintaining a network consisting entirely of employees is generally avoided as cost-prohibitive. As a result, runners may be employees of a particular commercial vendor or they may be independent contractors for one or more commercial vendors. ChoicePoint, for example, estimates that one-half of its court runners are its own employees, a figure it believes to be high for national players in the industry.[50]

(visited Jan. 20, 2004). Hereafter, About Rapsheets.

[45]Ibid.

[46]Walker article, *supra* note 27.

[47]ChoicePoint, Inc., "ChoicePoint® Acquires ASAP, Expands Capabilities in Tenant Screening," Press Release (Oct. 13, 2003) available at <www.choicepoint.com/choicepoint/news.nsf/newshome/?openform> (visited Jan. 20, 2004).

[48]*See* <www.nationalbackgrounddata.com/nbd/availablestates.cfm> (visited Apr. 2, 2004). Hereafter, NBD Criminal Record Searches.

[49]About Rapsheets, *supra* note 44.

[50]ChoicePoint, "ChoicePoint Comments to Draft DOJ/SEARCH National Task Force on the Role of the Private Sector in the Use and Management of Justice Information" (Feb.

Runners may be court employees earning extra money, former trial lawyers, law students, paralegals, or others. They may work full-time, part-time, or on an on-call basis. Some vendors require that the runners they hire have a business license and insurance. Court runners often specialize in records from a particular court or agencies in a particular county or counties. These runners become familiar with where to go to obtain records, how the court or agency organizes its records, and what the local court's or agencies' access policies and procedures are. In addition, runners, unlike the bulk record purchasers discussed later, are not limited to those courts and agencies that have automated their systems and make their records available in bulk. Furthermore, runners can obtain the most recent information available from the courts or agencies, unlike bulk data purchasers, who often can update records only on a monthly or other periodic basis.

As courts and agencies increasingly automate their recordkeeping systems and take advantage of the Internet as a means of distribution, it may be possible to search relevant records without sending a runner to the courthouse or agency. The Hamilton County, Ohio, court system, for example, has placed all of its publicly available records online. According to the Clerk of the Court, the site received 29 million hits in August 2002. He believes that "most of it is being used by attorneys, by landlords that are checking out potential tenants, by people checking out potential employees, and things of that nature," but estimates that 15% of users go to the site to find out about friends, relatives, or acquaintances.[51] In another example, Gwinnett County, Ga., near Atlanta, posts on a Web site the mugshot of anyone arrested in the county (approximately 14,000 per month), along with information about the charges filed.[52] Originally, records were to be publicly available through the site indefinitely, but following criticism on privacy grounds, the sheriff's department decided to limit public access to 31 days following arrest.[53]

Commercial vendors report that as a quality control measure, they frequently include "salted" requests among the requests they ask runners to fill. So-called salted cases are cases for which the commercial vendor already knows what records the court has on file in a particular matter. Given this knowledge, the vendor can review the records returned by the runner in order to confirm that a runner is checking all of the relevant sources and returning all the proper records.

Individuals and organizations that directly retrieve records from courthouses and government agencies have their own trade association, the Public Record Retriever Network (PRRN).[54] PRRN claims more than "700 members in 50 states that retrieve documents from local government agencies in over 2,000 counties nationwide."[55] The organization has a Code of Professional Conduct, which consists of 10 competency and client service guidelines.[56]

b. Bulk data purchases

With advances in automation, business models are changing. In the past few years, for instance, companies have begun purchasing records in bulk, particularly from State courts and corrections departments, and building their own databases for "instant" searches. Initially, these databases were

19, 2003). Hereafter, ChoicePoint comments.

[51]"'Dirty Laundry' on the web has some citizens very upset" transcript, *On the Record with Greta Van Susteren* (Sept. 5, 2002) (interview with Jim Cissell, Clerk of the Court, Hamilton County, Ohio). Hereafter, Dirty Laundry transcript.

[52]Matt Bean, "Mugshots online: Take a peek at the perps," CNN.com (Apr. 11, 2002) available at <www.cnn.com/2002/LAW/04/11/ctv.caughtonweb/> (visited Apr. 2, 2004).

[53]Ibid.

[54]Full membership in PRRN is open to "any firm or individual that physically goes to the county, court or other government agencies to search public records or retrieve documents. County coverage is limited to only those counties serviced with FICA-employees." Associate membership essentially "are public record database or gateway providers, public record distributors, or public record search firms that employ a correspondent network to obtain records." BRB Publications, "The Public Record Retriever Network," available at <www.brbpub.com/prrn/prrn_info.asp> (visited Jan. 20, 2004).

[55]Ibid.

[56]Ibid. The competency guidelines include: 1) knowing where each type of local public record is located; 2) accessing these records regularly; 3) understanding the content of the records retrieved; 4) searching the records themselves in those government agencies that do not conduct searches for the public; and 5) maintaining good relationships with agency personnel. The client service guidelines include: 1) returning calls promptly; 2) completing projects as promised; 3) explaining charges in advance; 4) expediting results on request; and 5) on request, explaining how agencies maintain their records. Ibid.

designed and marketed to serve narrow searches limited by county or State.

Beginning in 2001, however, commercial vendors began to rollout "nationwide" products. These products allow users to almost instantly search proprietary databases containing upwards of 160 million criminal records from every State. As such, these searches provide nearly instant access to a far greater breadth of information that does not focus merely on jurisdictions where an individual most recently lived or worked. One drawback, however, is that the currency of the data contained in these databases may vary widely, depending on how frequently updates are available from State and local courts and agencies and how frequently these updates are obtained by the commercial vendor.

2. More on bulk purchases of criminal justice information

Whether a court or agency sells its records in bulk depends on local law and the policies of the court or agency. Bulk data purchases typically consist of the transfer of electronic, rather than manual, records.[57] When information is purchased in bulk from public record sources, it is standard practice for commercial vendors to maintain information from each data source separately (although multiple databases may be indexed to facilitate a multisource search). This allows the vendor to offer its customers searches of particular data sources or combined queries.

To facilitate the ability to search multiple databases with one query, the records obtained from courts and State agencies are typically "normalized" (that is, converted into the vendor's standard format) before being made available to end-users. Normalization can be a difficult undertaking because the formatting and structure of databases can vary from court to court and agency to agency. Task Force members noted that it is not uncommon for the descriptions of offenses used by prosecutors, the courts, and repositories in a particular State to vary. In addition, offenses, offense codes, and offense descriptions included can vary widely from State to State, and these variants must be accounted for during the normalization process.[58]

During the normalization process, some vendors screen out information that they do not believe is relevant to any of the purposes for which their customers are obtaining reports. One member of the Task Force noted, for example, that while some of the bulk data that his company receives includes military service history and next of kin information, that information is not included in reports that are ultimately provided to end-users.

Formats in which bulk data are provided to commercial vendors vary widely, based on the technical capabilities of the court or agency providing the data. For example, data may be transferred to vendors via CD-ROM, ZIP files, floppy disks, or magnetic tapes.

Updates are typically available on a monthly basis. This varies, however, depending not only upon how often the source makes updates available, but also on whether the vendor promptly obtains the update and integrates it into existing products. Updates may include only new records or they may also include updated or deleted records. As a result, vendors customarily prefer to obtain an entirely new copy of the database because this relieves the vendor of having to merge a small subset of updates into an existing system.

Bulk ordering and invoicing practices vary by court or agency. In some cases, once an account is established, updates are automatically sent along with an invoice. In other cases, the commercial vendor must be proactive, submit-

[57] One possible exception is police blotter information, which is typically not automated. As a result, users, such as reporters, must rely on manual records.

[58] The Joint Task Force on Rap Sheet Standardization, comprised of representatives of the FBI's Criminal Justice Information Services (CJIS) Division, the CJIS Advisory Policy Board (CJIS APB), the National Law Enforcement Telecommunications System (NLETS), SEARCH, and State and local law enforcement agencies, has been working since the mid-1990s to develop a standardized interstate criminal history specification. The principal objectives of the project are to develop an XML-based standardized criminal history transmission format; develop a standardized presentation format utilizing the XML transmission format; and develop a concept of operations that combines criminal histories from multiple jurisdictions into a similar criminal history. Joint Task Force on Rap Sheet Standardization, *Interstate Criminal History Transmission Specification: XML Version 2.01* (June 2001) at p. 4. Once completed and implemented, this standardization effort would benefit not only the criminal justice community, but also commercial vendors by reducing the normalization burdens they currently face.

ting orders and payments to the court or agency, which subsequently sends the data.

3. Compiler versus reseller

Another distinction among commercial vendors turns on whether the vendor obtains its information from a governmental source or obtains the data from another commercial vendor. Commercial vendors that obtain information compiled by other commercial vendors for the purpose of reselling the data are generally referred to as "resellers." The Federal Fair Credit Reporting Act[59] imposes special obligations on resellers (if the report being sold constitutes a "consumer report") in recognition of their unique status as middlemen between the compiler and the end-user.

Frequently, commercial vendors act as both compilers and resellers, compiling products in their area of specialty, while reselling other information products. Rapsheets.com, for example, specializes in compiling criminal justice information. It also, however, acts as a reseller of name, address, and Social Security number identification and verification products produced by Experian and TransUnion.[60]

4. Customer base

Another distinction among commercial vendors is the manner in which they market their products. Some vendors, such as National Background Data, do not sell their products directly to end-users, such as employers and landlords. Instead, they serve solely as a source of information for background screening companies that then resell the information to end-users. Other vendors sell their products both directly to end-users and through resellers. Some commercial vendors target end-users who are looking to use reports for particular purposes, such as employment screening, while others make the information available to any type of end-user, including the general public.

5. Prices

a. Factors impacting vendor pricing

From all accounts, the prices that commercial vendors charge for criminal justice information vary widely. Broadly speaking, price is a function of the cost of the records being sought and the amount of resources that commercial vendor must employ to prepare the report.

Factors influencing price might include the method of research employed, and the extent to which the vendor (as opposed to the end-user) analyzes the results. Online research is generally less expensive than sending runners to courthouses. Similarly, the less analysis required by the commercial vendor, the less expensive the report usually is for the customer. For example, a report that provides the consumer with all the information collected by the vendor (and which the consumer is responsible for evaluating), is generally less expensive than a product in which the commercial vendor (1) applies the customer's hiring criteria to information produced in the course of a background check, then (2) makes a recommendation regarding placement of the report subject. The type of report ordered also can have accuracy and relevancy implications.[61]

[59] 15 U.S.C. § 1681 et seq. The FCRA is discussed in part II of this report.

[60] Rapsheets.com, "Other Searches," available at <www.rapsheets.com/rapsheetsnm/othersearch.asp> (visited Jan. 20, 2004).

[61] This point was made in a submission to the Task Force by ChoicePoint: "In general, the use of static databases or online access to court indexes can be provided rapidly at a very low price, however the relevance and accuracy of the information provided may offset the initially perceived value. Conversely, the most accurate method of criminal record retrieval may be through an in-person review of actual court docket records, however this service is typically more time consuming and expensive. The vendor's review and handling of criminal record information before delivery to the client will also affect pricing. Clients who retrieve records through direct vendor access are usually provided raw data or record information. This type of service results in a low acquisition cost for the client but requires additional effort by the client to validate the accuracy of the record and its connection with the subject. At the other end of the spectrum are clients who require only a Pass or Fail result from their vendor, with the vendor responsible for confirming the record belongs to the subject and for using the client's decision matrix to judge if the record found is acceptable or unacceptable." ChoicePoint comments, *supra* note 50.

There may also be other factors at play in pricing, such as the number of background checks that a vendor orders (which may warrant a volume discount) and the actual cost of obtaining data from a particular source. In addition, what a particular target market is willing to pay for the product being provided can also be an important factor in pricing.

Table 1 illustrates how data sources and vendor services can affect the price of the report produced.[62]

Table 1: How vendor services affect report prices

	Data source		
Vendor service level	**Static database or court index searches**	**Online record searches through State-level access**	**In-person record review**
Direct data access with no adjudication or analysis of records	$	$	$$
Record review to confirm match with subject	$	$$	$$
Record review to confirm match with subject ***plus*** filtering of nonemployment records	$$	$$	$$$
Record review to confirm match with subject ***plus*** pass/fail scoring based on client's decision matrix	$$	$$$	$$$

[62]Source: ChoicePoint, Inc.

b. Vendor pricing examples

Some vendors advertise pricing on the Internet. It is not always possible to tell from the sales materials whether the information is being drawn from databases or through the use of runners; however, it is reasonable to assume that instant or nearly instant statewide or national searches are database searches. Local or county searches could be compiled using runners or through databases. Examples, current as of January 2004, include:

- YourOwnPrivateEye.com charges $295 for a "nationwide" criminal search and $45 for a "comprehensive statewide criminal check," the results of which are e-mailed to the purchaser "within 24 hours."[63]
- US Search, a First Advantage Corporation, advertises on television and sells reports via the Internet and a toll-free number. US Search's charges for statewide criminal checks range from $59.95, depending upon the State. Onsite county court checks cost $29.95 per county. Results are returned in 7–10 days.[64]
- CheckMate bills itself as the "original online background service designed especially for dating singles."[65] Checkmate's criminal checks range in cost from $25 to $29 per jurisdiction for county, State, and Federal district searches.[66]
- BackgroundChecks.com is an Irving, Tx., company established in 1999. The firm offers "instant" database background checks for 45 States, with prices ranging from $5 to $12 for individual State searches and $13.95 for a 45-State search, with monthly plans available for high-volume users. [67]
- Rapsheet.com's searches for consumers range from $29.95 for a search of its entire 160-million record "National Criminal Index," $14 for a regional search, $10 for a single-State search, and $5 for a search of more than 30 sex-offender registries.[68] Businesses, which pay a $14.95 monthly fee, pay $19.95 for a "National Criminal Index" search, $8 for a regional search, $6 for a State search, and $3 for the sex-offender registry search.[69]
- ChoicePoint charges $25 for a pre-employment search of its 90-million record National Criminal File and $5 for a State criminal database search through its ScreenNow.com Internet site.[70] Sex-offender registry searches are $9. Special screening packages for volunteer organizations are priced from $2 to $9, depending upon the jurisdiction, with additional State or county expenses in some cases.[71]

c. Point of comparison: Report pricing from State criminal history repositories

Some State criminal history repositories are authorized to make their criminal history records available to the public at large or to certain authorized users, such as schools, nursing homes, etc. According to a 2001 SEARCH survey, fees charged by the repositories ranged from $2 to $49, depending upon the requester and whether the check is a name-plus-identifier check or a fingerprint-based check. Many States waive or reduce background check fees for nonprofit organizations that deal with vulnerable populations such as children, the disabled, and the elderly.[72]

In Florida, for example, a State name-plus-identifier check available to the general public and conducted through the Florida Department of Law Enforcement costs $23, while a national, fingerprint-based check for authorized users costs $36 for volunteer

[63]YourOwnPrivateEye.com, "Criminal Records," available at <www.yourownprivateeye.com /criminal.htm> (visited Jan. 20, 2004).

[64]US Search, "Consumer Services," available at <www.ussearch.com> (visited Jan. 20, 2004).

[65]*See* <www.checkmate1.com/> (visited Jan. 20, 2004).

[66]CheckMate, "Background Checks," available at <www.checkmate1.com/checkmate prices.htm> (visited Jan. 20, 2004).

[67]BackgroundChecks.com, "Pricing," available at <www.backgroundchecks.com> (visited Jan. 20, 2004).

[68]Rapsheets.com, "Pricing," available at <www.rapsheets.com/comsumer /pricing.asp> (visited Jan. 20, 2004).

[69]Ibid.

[70]ChoicePoint, "Pricing," available at <www.employment.screennow.com /hdocs/pricing.html> (visited Jan. 20, 2004).

[71]ChoicePoint, "State-Specific Background Screening Packages," available at <www.volunteerselect.com/hdocs /packages.html> (visited Jan. 20, 2004).

[72]SEARCH, "Survey of states that provide some level of 'open' access to their criminal history record" (Mar. 27, 2001) at p. 1, available at <www.search.org>. Hereafter, SEARCH repository survey.

organizations and $47 for most other requestors.[73] In Oklahoma, name-plus-identifier checks can be obtained through the Oklahoma Bureau of Investigation for $15 and fingerprint checks can be obtained for $19.[74]

6. Identification/Record matching

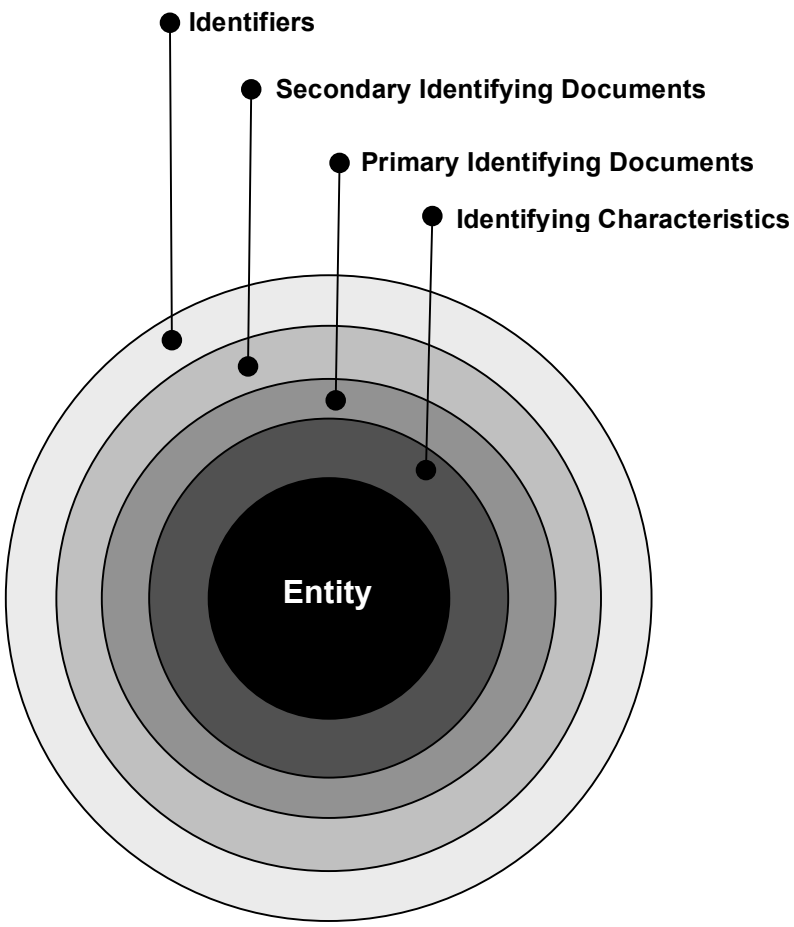
a. Establishing identity

Identity is more than name alone. As the National Electronic Commerce Coordinating Council has explained in the course of its e-commerce work:

> Clearly, the concept of identity is far broader than the content of a name. While names and naming protocols are a critical element of identity, in that they give us the means to call out one identified individual from another, the underlying relevance, role, context, and meaning attributed to a given named person can only be gleaned by reference to other factors. The full measure of identity of an individual is a subtle and multifaceted complexity. This is because people exist in many social, economic, political, cultural, and other dimensions all at once. In short, one size does not fit all when it comes to the identity of a person.[75]

The interrelation of these "other factors" is illustrated by the following diagram (figure 1).[76]

Figure 1: The concept of identity contains multiple layers



[73] *See* <www.fdle.state.fl.us/Criminal History/> (visited Jan. 20, 2004).

[74] *See* Oklahoma State Bureau of Investigation, "Frequently Asked Questions: How Much Does a Criminal History Record Check Cost?," available at <www.osbi.state.ok.us/FAQs.htm> (visited Jan. 20, 2004).

[75] *Identity Management: A White Paper* (Lexington, Ky.: National Electronic Commerce Coordinating Council) presented at the NECCC Annual Conference, Dec. 4–6, 2002, New York, NY, at p. 27. Available at <www.ec3.org/Downloads/2002/id_management.pdf> (visited June 28, 2004).

[76] Ibid., at p. 43 (Appendix A: Glossary of Terms, by Ed Fraga).

At the core is the entity, which, in the criminal justice context, is the individual who is interacting with the criminal justice system. At the outer edge of the spectrum are identifiers—such as names, numbers, and titles—that can be asserted and readily claimed and changed by individuals.[77] In between, are various means of linking identifiers with an entity. Moving from the core to the outer edge, each successive level becomes less integrally associated with the individual. Identifying characteristics—such as fingerprints, other biometrics, or other unique characteristics associated with an entity—are most closely linked to the entity. Primary identifying documents "link an identifier with an entity often by association with an identifying characteristic such as a fingerprint."[78] Secondary identifying documents reference identifiers without relying on an identifying characteristic.

Identifying characteristics are a valuable means of linking identifiers to an individual because they are uniquely linked to the individual. The value of identifying characteristics as a means of determining identity is, however, only as strong as the enrollment process used to associate identifiers with an identifying characteristic and the individual. When the State or a person with whom the individual does not have a personal relationship seeks to match a claimed identity with the individual, they often rely upon primary or secondary identifying documents to "verify" identity and link the identity to the individual.

Identity verification (also referred to as "identity authentication") has become increasingly important over the past several years in light of the rise of identity theft and concerns about terrorism. These concerns have prompted both governments and the private sector to seek ways to improve identification documents and otherwise authenticate that an individual is (or is not) who he or she claims to be through biometric or other means.

The effort to curb identity theft has produced conflicting strategies regarding the use and availability of personal information. Since personal information, such as the Social Security number, can facilitate identity theft, one approach has been to try to curtail access to this information (by excluding it from public records, for example). Conversely, a number of private-sector initiatives have resulted in identity authentication products that rely on more personal information and/or sophisticated modeling tools in an effort to curb identity theft.

Some companies have created identity authentication products that rely on so-called "out-of-wallet" data to authenticate someone's identity. The information has been dubbed "out-of-wallet" data because it relies on information that is likely to be known to the actual consumer to whom it pertains, but would not typically be known to a criminal who stole the individual's wallet (as could be the case with a driver's license number, Social Security number, date of birth, etc.). A consumer, for example, might be asked questions about the amount, size, or holder of his or her mortgage, the amount paid for his or her home, or other such information.[79]

Another company, ID Analytics of San Diego, has developed a pattern-recognition technology designed to assess "the legitimacy of identity information provided by individuals to find signs of fraud."[80] The product, Graph Theoretic Anomaly Detection, is an algorithm that seeks to "detect unusual patterns based on the identity elements on an application."[81] The algorithm was developed based on an analysis of information from 200 million applications for products and services from 13 companies, including credit card issuers, online retailers, and wireless telephone service providers. Once the algorithm has been applied to an application, a score is produced signifying the risk of identity fraud.[82]

---

[77]Individuals can claim various identities (aliases). The term "alias" often has a negative connotation because it is frequently used in the context of an individual who has asserted multiple identities for the purposes of deception or evasion for illicit purposes. It is important to note, however, that people may have multiple identities in the course of their everyday lives. *See, for example,* ibid., at p. 36.

[78]Ibid., at p. 43.

[79]Chris Costanzo, "Special Report: Retail Delivery, Using Technology to Thwart Identity Thieves" American Banker Online (Nov. 18, 2003) available at <www.idanalytics.com/news_and_events/abo20031118.html> (visited Apr. 2, 2004). Hereafter, Costanzo article.

[80]ID Analytics, "AMS and ID Analytics to Help Government Clients Fight Fraud" (Dec. 15, 2003) available at <www.idanalytics.com/news_and_events/20031215.html> (visited Apr. 2, 2004).

[81]Ibid.

[82]Costanzo article, *supra* note 79.

b. *Identity in the criminal justice context*

Not surprisingly, individuals do not always provide law enforcement with correct identifiers when they interact with law enforcement (sometimes relying upon falsified or fraudulently obtained primary or secondary identification documents). The criminal history repositories address this problem by organizing their records around an identifying characteristic such as the fingerprint. The repository's criminal history record therefore stands for the proposition that an entity (individual) with this identifying characteristic (fingerprint) interacted with the criminal justice system with respect to the listed offenses. The criminal history record also includes any identifiers asserted by the individual, including whatever name(s) the individual has claimed.

Fingerprints have not been associated with every record generated by the criminal justice system, however. Customarily, fingerprint checks have been time-consuming and expensive. In addition, fingerprints are not always included with records, because individuals are not fingerprinted for all offenses. In addition, most court and corrections records do not carry the individual's fingerprints, instead referencing the individual by name and perhaps other descriptors, such as date of birth, address, Social Security number, or physical description. Furthermore, in the commercial-vendor context, fingerprint-based checks are usually unavailable due to a lack of access to repository records. Additional reasons that commercial fingerprint-based screening efforts have lagged are resistance to fingerprinting by end-users as a result of cost concerns, time concerns, or concerns that the individual whose background is to be checked would object to providing the prints.

As a result of the foregoing factors, commercial vendors (and State repositories in some instances) customarily conduct name-plus-identifier checks (sometimes referred to simply as "name checks"). The term "name-plus-identifier check" is shorthand for a check that does not base identification on fingerprints or other biometrics, but instead relies on an individual's name, as well as other descriptors, such as date of birth, current and former addresses, Social Security number, places of employment, or other facts.

When a name-plus-identifier check is conducted, there is a possibility that a background check of an individual with a criminal history will produce no results because the individual is asserting a stolen or fabricated identity (a "false negative").[83] It is also possible that a check of an innocent person's background will produce a false positive because some or all of his or her identifiers match the identifiers used by the individual who actually interacted with the criminal justice system (either because the two actually share certain identifiers or because of identity theft).

In Minnesota, for example, a woman filed suit against the State Bureau of Criminal Apprehension (BCA) for failing to remove her name from a conviction record that resulted from an identity thief's use of her name as an alias.[84] The innocent woman had an apartment rental application declined on the basis of her purported criminal record.[85] The BCA used a fingerprint test to confirm that the woman was not the person arrested for the crime, but refused to remove the information, contending that it must keep the information on file in case the identity thief attempts to use the alias again. According to the woman, the BCA gave an unsigned letter to her, which she could present to potential landlords or employers, stating that no convictions could be found based on a search of her name, date of birth, and fingerprints.[86] In another instance, a law school graduate was handcuffed and jailed in San Diego when she showed up for her first day on the job because a "background check had uncovered a warrant for her arrest for possession of marijuana, but the actual fugitive was a thief who had stolen her wallet and assumed her identity."[87]

[83]Commercial vendors have developed a variety of products designed to detect false identities, such as products designed to validate Social Security numbers. Also, it is important to note that false negatives can occur (even in fingerprint-supported situations) as a result of other factors. For example, a false negative may occur if a prior interaction with the justice system occurred in a jurisdiction not covered by the background check or if the offenses that occurred are not included in the records systems that are searched during the background investigation.

[84]Hannah Allam, "St. Paul Victim of ID theft sues BCA," *St. Paul (Minn.) Pioneer Press* (Mar. 23, 2002). Hereafter, Allam article.

[85]It is unclear from media reports whether the landlord conducted the background check in question through a commercial vendor or went to the BCA directly.

[86]Allam article, *supra* note 84.

[87]Eve Tahmincioglu, "Tense Employers Step up Background Checks,"

c. *Vendor practices with respect to name-plus-identifier checks*

When conducting a name-plus-identifier check for criminal background check purposes, industry practices vary with respect to what information about the record subject either may or must be supplied in order to run the check.

Commercial vendors seek to reduce the possibility that a false positive will be produced as a result of a name-plus-identifier check by relying on multiple identifiers to match a background check subject with criminal justice record information. For example, as ChoicePoint informed the Task Force:

> ChoicePoint has Standard Operating Procedures regarding the reporting of criminal activity [in its information products]. There must be a minimum of two identifiers in order to report the record information. These identifiers are most commonly the name, date of birth, and the Social Security Number. Additional identification information can include a driver's license number or a residential address. A physical description can assist in eliminating false positives when State and county repositories provide that information.[88]

ChoicePoint uses two internal groups to review the information before it is returned to the party that ordered the report.[89]

As noted previously, commercial vendors are developing new products designed to rely upon nontraditional identifiers and behavior patterns to authenticate that an individual is the person claimed. The utility of these new products for purposes of validating the criminal justice information obtained from court records or other public sources is potentially limited, however, because these records may include only a minimal amount of personal information about the individual that could be used for purposes of matching a particular person with the record.

d. *Vendors and fingerprint-based checks*

Customarily, end-users who order criminal background checks for pre-employment or residential housing screening as part of their due diligence rely almost exclusively on name-plus-identifier searches.[90] The principal exception consists of end-users who are authorized or required to conduct fingerprint-based checks through the State repository system or the FBI.

Traditionally, commercial vendors have not been able to play a significant role when end-users, principally employers, are willing and statutorily able to run fingerprint-supported background checks through the State repositories or the FBI. There are signs, however, that this may be changing. ChoicePoint's "Employee and Applicant Fingerprint Solution" (EAFS), for example, "helps organizations collect, authenticate, and transmit personal and biometric data more efficiently."[91] The application can be integrated with livescan devices or a personal computer coupled with an FBI-approved desktop scanner. In addition to facilitating the transfer of biometric information to the relevant Federal or State agency, ChoicePoint also "verifies the identity of the people you fingerprint prior to the submission of the fingerprints to Federal or State agencies."[92] In addition, ChoicePoint offers customers the opportunity to search its National Criminal File prior to submitting the fingerprints to State or Federal agencies.[93]

In another sign that the traditional lack of involvement by commercial vendors may end, the Compact Council—established by the National Crime Prevention and Privacy Compact of 1998 to set rules, procedures, and standards for fingerprint-based, noncriminal justice criminal history checks—issued a notice in the *Federal Register* of its intent to issue a rule allowing the outsourcing of administrative functions pertaining to background checks for authorized noncriminal justice purposes.[94] In its notice, the Compact

New York Times (Oct. 3, 2001) available at <www.nytimes.com>. Hereafter, Tahmincioglu article.

[88]ChoicePoint comments, *supra* note 50.

[89]Ibid.

[90]Robert W. Holloran, et. al., *Standards for the National Background Directory* (Ocala, Fla: National Background Data, July 21, 2001) available at <www.nationalbackgrounddata.com/pdf/national_background_directory_standards.pdf>. (Visited June 28, 2004).

[91]ChoicePoint, "Employee and Applicant Fingerprinting Solution," available at <www.choicepoint.net/choicepoint/industry/financial/eafs.html> (visited Apr. 2, 2004).

[92]Ibid.

[93]Ibid.

[94]68 *Federal Register* 9098 (Feb. 27, 2003).

Council cited the escalating demand for fingerprint-based criminal history record checks for noncriminal justice purposes and a resulting increase in workload for government agencies and nonprofits as the principal reason for the change.[95] Such a rule change could further encourage the private sector to develop the infrastructure necessary for the processing of fingerprint-based criminal checks.

D. End-uses of criminal justice record information obtained from commercial vendors

"Hard" statistics are unavailable, but it is the sense of the Task Force that the overwhelming majority of criminal background checks that commercial vendors conduct are for purposes of employee, volunteer, and tenant screening. It is the further sense of the Task Force that media inquiries constitute a significant portion of the remainder. The remainder of the criminal background check market is small, but there are many other purposes for which criminal justice information is obtained from commercial vendors, ranging from fraud investigations to idle curiosity.

1. Employment screening

Thirty or 35 years ago, employment background checks were relatively rare, typically limited to high-ranking or particularly sensitive positions. Today, however, amid concerns about issues ranging from terrorism to child abuse, employment background checks are far more common. Employment background checks are most common during the hiring process. Investigation or reinvestigation of current employees also may occur, however, particularly where there is a need to (re)validate security clearances or when there is a promotion, new assignment, potential misconduct, or other important event.

This is particularly true of employees who come into contact with children, the elderly, or other vulnerable populations. Even Santa and his elves are subjected to criminal background checks (and drug tests). According to an official with Santa Plus, a division of Eastman Kodak that places shopping mall Santas, conducting criminal background checks is routine. One commercial vendor found that about 70 of 1,000 shopping mall Santa and Santa's Helper applicants had committed crimes in the past 7 years, including indecent exposure, solicitation of prostitution, and drunk driving.[96]

There are numerous reasons for using a commercial vendor for employment screening. In some cases, it is simply a matter of convenience, because the employer lacks the time or the know-how to obtain the relevant information directly from a court or other government source. In other cases, the position for which the employer is conducting a criminal background check is not one for which access to State repository information is authorized by law.

In some cases, even if a fingerprint-based check is legally required—effectively assuring that the check is processed through the State repositories or the FBI—employers still may use a commercial vendor to conduct a less expensive "pre-check." If disqualifying results are returned, the candidate may be eliminated from consideration without a lengthy or more expensive check through the State repository or the FBI.

In addition, some employers eligible to conduct checks through the State repositories or the FBI use commercial vendors to supplement the information provided in those reports by having the vendors conduct checks of the records at local courthouses.

2. Volunteer screening

Over the past 10 to 15 years, volunteer organizations have begun to order many more background checks of their volunteers. This is particularly true of volunteers who come into contact with children, the elderly, or other vulnerable populations. The National Child Protection Act of 1993 and numerous State laws have authorized the use of the FBI and State repositories to conduct checks for many of these positions. Volunteer organizations, however, frequently rely on private vendors to conduct these checks because of cost concerns and time considerations. The Boy Scouts, for example, has hired ChoicePoint to conduct criminal checks on all of its new volunteers.[97] According to a Boy Scouts spokesman, the requirement, at least initially, would apply only to new adult volunteers, not the 1.2 million existing volunteers.[98]

[95]Ibid.

[96]Associated Press, "Santas Undergo Background Checks," AP Online (Nov. 25, 2002).

[97]Ira Dreyfuss, "Boy Scouts plan checks for future volunteers," *Boston Globe* (Nov. 28, 2002).

[98]Ibid.

While the Boy Scout program is designed to apply, at least initially, only to new rather than existing volunteers, the ability to "recheck" volunteers at periodic intervals is an important consideration for volunteer organizations, particularly those that have volunteers who interact with vulnerable populations.

3. Tenant screening

Landlords, particularly large property management companies, routinely order criminal background checks on potential tenants. For certain Federal housing programs, background checks are required to qualify or retain eligibility.[99]

The amount and extent of criminal justice record information that can be relied upon by the rental housing industry varies widely by location, based on variations in local housing nondiscrimination laws, which can affect the extent to which a landlord can refuse to rent to someone merely because of a criminal record.[100]

4. Media

It is a longstanding custom of media outlets to obtain criminal justice information directly from the courts, police blotters, and other sources in the course of reporting on recent arrests, ongoing trials, criminal appeals, pardons, and paroles. Many newspapers, of course, establish and use "news morgues," which are manual (and, more recently, automated) criminal justice information systems. Today, media outlets may also use commercial vendors to obtain criminal justice information about individuals who are the subject of news stories.

5. Immigration-related checks

Some commercial vendors see immigration-related checks about foreign nationals as an especially promising market.[101] One aspect of this potential market is the monitoring of criminal activity in the United States by visa holders. Another aspect is determining whether immigrants have committed offenses that merit their deportation from the United States.

---

[99] *See, for example,* 66 *Federal Register* 28776 (May 24, 2001) (Department of Housing and Urban Development regulations mandating criminal background checks for certain public housing residents).

[100] Allowing for variations as to what is legally permitted, the rental-housing industry appears to view felony information as being of primary importance in tenant screening. A collective effort by the apartment industry to create shared data standards, for example, has resulted in the development of a standard for tenant screening through the National Housing Council's Multifamily Information and Transactions Standards (MITS) project. The voluntary standard includes fields for the entry of felony information about applicants, including whether the applicant has ever been convicted of a felony, the date of the felony conviction, and a "narrative description of the felony conviction." MITS, "Apartment Industry Data Standard Initiative Releases Version 1.0," Press Release (Nov. 25, 2002) available at <www.nmhc.org/Content/PressRoom/Index.cfm?Year=2002> (visited June 28, 2004); MITS, "Data Element Dictionary" (undated) available in the "Current Specifications" section at <www.mitsproject.com>.

[101] The private sector, particularly employers, is also interested in information about immigration status because of the implications of immigration status for eligibility for employment and government benefits. The Bureau of Citizenship and Immigration Services (BCIS) has developed a program to facilitate access to certain immigration status information. The Bureau's Systematic Alien Verification for Entitlements (SAVE) program facilitates access to the Bureau's Alien Status Verification Index (ASVI), which contains selected immigration status information on over 60 million records.

"The SAVE program enables Federal, state, and local government agencies to obtain immigration status information they need in order to determine applicant's/recipient's eligibility for many public benefits." U.S. Immigration and Customs Enforcement, "Immigration," available at <www.ice.gov/graphics/enforce/imm/> (visited June 28, 2004).

In addition, the SAVE program has launched pilot programs in several States to "enable employers quickly and easily to verify the work authorization of their newly hired employees." The basic pilot program, which is being conducting by the BCIS and the Social Security Administration (SSA) in the States of California, Florida, Illinois, Nebraska, New York, and Texas, allows employers to conduct verification checks of SSA and BCIS databases for all newly hired employees, regardless of citizenship. A second pilot program, the Citizen Attestation Pilot, is being conducted by BCIS alone in Arizona, Maryland, Massachusetts, Michigan, and Virginia.

Both pilot programs are free to employers, who must execute a memorandum of understanding that lays out restrictions on the ability of employers to use and disclose the information. Use of the system, for example, is limited to newly hired employees; it is not to be used as a prescreening tool or as a means of checking the status of existing employees. U.S. Citizenship and Immigration Services, "SAVE Program," available at <http://uscis.gov/graphics/services/save.htm> (visited June 28, 2004).

Commercial vendors can act as authorized agents of employers for the purpose of participating in this program, thereby facilitating employer participation in the program.

6. Fraud investigation or prevention

Insurers and many others in the private sector use criminal justice information as a part of fraud investigations or prevention activities. An insurer, for example, may obtain criminal justice information in the course of reviewing a claim to determine whether a claimant has a history of fraud that may merit a closer look at the claim. In some cases, the criminal justice record information may be incidental to the investigative use. Insurers, for example, may use criminal driving record information to identify drivers in a household who have not been listed on automobile insurance applications.

7. Licensing

In a variety of circumstances, criminal background checks are required for business, professional, and occupational licensing purposes. These checks are usually conducted through State criminal history repositories or the FBI rather than commercial vendors, although State licensing boards may conduct background checks through commercial vendors in some instances.

In addition, in some cases where State or Federal licensing is prerequisite for employment in a particular profession, an employer may elect to conduct a "precheck" of an applicant through a commercial vendor before submitting the application to the licensing agency.

8. Due diligence

Due diligence investigations in mergers, acquisitions, and other commercial transactions often prompt criminal background checks of officers or employees of a prospective business partner. In some instances, entities in highly regulated industries, such as the gaming industry, must conduct criminal background checks on prospective vendors and business partners because doing business with a vendor with a criminal record could impact their licensing status. Criminal justice information is also relevant in other business relationships, including efforts by financial institutions and other businesses to "know" their customers.

9. Prenuptial analysis

In an increasingly "risk-averse" world, some individuals even order criminal background checks on dating partners or prospective spouses. As the president of one commercial vendor said when describing his company's offerings, "[Our] service is a tool not only for corporate users … If your daughter was going on a date with someone for the first time, there is no reason you can't check the guy out."[102] In fact, some online vendors specialize in this market. One Texas company, CheckMate, bills itself as the "original online background service designed especially for dating singles."[103]

10. Marketing

In some cases, criminal justice information, particularly name and address information associated with recent arrests, is used to market services related to the criminal justice system, such as bail bond services, attorneys, driving schools, religious counselors, and drug and alcohol counselors.[104] Customarily, this niche market is occupied primarily by local, rather than national, commercial vendors.

11. Accountability

In some cases, individuals order criminal background checks to confirm that government or private-sector employees have been vetted properly, particularly those who deal with children. Parents may seek a background check on a school bus driver or daycare worker because they are interested in knowing whether the school district or daycare center did a good job of vetting the employee. Similarly, public interest groups may order a criminal background check on political appointees to ensure that they are eligible or otherwise suitable to hold the position to which they are being appointed.

12. Litigation research

Lawyers may conduct criminal background checks on parties to litigation, prospective witnesses, or prospective jurors in order to assess the credibility and suitability of individuals.

---

[102] Walker article, *supra* note 27 (quoting Peter Schutt, President of Rapsheets.com).

[103] *See* <www.checkmate1.com/> (visited Jan. 20, 2004).

[104] These types of service providers were all customers of United Reporting Inc., a commercial vendor that obtained recent arrest information from police departments, such as the Los Angeles Police Department. In 1996, when California changed its law prohibiting commercial access to this arrest data, United Reporting challenged the statute on first amendment grounds. United Reporting ultimately lost its case when the Supreme Court upheld the statute in a 7-2 decision. *Los Angeles Police Dept.* v. *United Reporting Publishing Corp*., 528 US 32 (1999).

13. Opposition research

Political campaigns use criminal justice records to identify the potential vulnerabilities of their candidates, as well as the potential vulnerabilities of their political opponents.

14. Voter eligibility

Customarily, a felony conviction makes an individual ineligible to vote. Election officials may rely on private companies to verify the eligibility of individuals on its voting roles.

15. Curiosity

In some instances, criminal background checks are ordered by individuals who are simply curious about their friends, neighbors, or relatives.

16. Registered traveler programs

In the wake of the September 11 terrorist attacks, air travel has changed. Today, Americans are subject to new identification and search procedures at every commercial airport. While these procedures are necessary—and, indeed, research shows that they are widely supported by the American public—they are also inconvenient, time consuming for the public, and expensive for taxpayers.

As one part of an effort to meet these concerns, Congress has authorized the Transportation Security Administration (TSA) to develop a trusted traveler program. TSA is currently conducting pilot tests of trusted traveler model programs at several airports.

Eventually, it is expected that the program will be run by the airlines or other private companies. There are several core elements to the trusted traveler program:

- Participation in the program will be voluntary.
- The first step in enrolling in the trusted traveler program will be a relatively rigorous process of identification verification.
- Once enrolled, trusted travelers will provide a biometric (most likely, a fingerprint) that will be maintained in a database and used to compare with the "live" biometric to make positive identification.
- A criminal history background check will be a required condition of enrollment.
- A check against various "no-fly," "selectee" and other watch lists will also be a required element.
- Participation in the trusted traveler program will require periodic updates of the criminal history check and the "watch list" check.

The hope is that trusted traveler programs will not only contribute to security, but will also make for a faster and more convenient trip through airport security lines. If the trusted traveler programs prove to be popular, it is certainly conceivable that over 100 million adult Americans will participate. This means 100 million criminal history record searches will be requested, not even counting periodic updates. The trusted traveler programs could well be a catalyst for the most dramatic and immediate surge in the number of criminal history record checks in the Nation's history. Many experts predict that commercial vendors must, and will, play a key role in trusted traveler programs, in general, and criminal history record searches, in particular.

E. Sources of criminal justice record information for commercial vendors

Criminal justice record information "originates" from law enforcement agencies, the courts, corrections agencies, and prosecutors. State criminal history repositories and the FBI's National Crime Information Center (NCIC) are, technically, secondary sources. Which sources a particular commercial vendor relies upon, however, vary by State because State law customarily does not allow noncriminal justice users to have access to all information sources for all purposes. In many States, commercial vendor access to information maintained by the State criminal history repository customarily has been restricted. As a result, information is often obtained from courts and corrections agencies. The mix of data sources used by a commercial vendor may vary over time as new sources of data (particularly bulk data) become available.

Which sources a particular vendor relies upon may also vary, depending upon the vendor's business model. For example, if a particular court or agency does not make its information available in bulk, its records are apt to be relied upon by only those vendors with the capability to provide traditional reports.

Even if records are available from a court or agency, the cost of the records may be prohibitively high. In some cases, for instance, bulk

purchase of repository data is not cost-effective. In Florida, for example, no bulk discount for repository data exists.[105] Therefore, for a commercial vendor to purchase the roughly 13 million records held by the Florida Department of Law Enforcement (FDLE), the vendor would need to pay the State's standard $23-per-search charge.[106]

1. The courts

The primary source of criminal justice information for commercial vendors is the court system. During 2001, more than 14 million criminal cases were filed in State trial courts and nearly 63,000 in the Federal district courts.[107] "Fifteen States each reported over 100,000 criminal filings, collectively accounting for three-fourths of the total general jurisdiction criminal filings."[108] California reported the most filings, with 742,582, while Alaska reported the fewest, with 3,337.[109]

The structure of State court systems is not uniform nationwide, and this very much impacts the manner in which commercial vendors may obtain court data, particularly bulk data. State court systems are large and diverse, with more than 16,200 State trial courts, including more than 13,600 courts of limited jurisdiction (authorized to hear only certain types of cases) and more than 2,500 courts of general jurisdiction.[110] Thirteen States have adopted a unified trial court structure, meaning that courts are consolidated into a single general-jurisdiction court level with jurisdiction over all cases and procedures.[111] The remaining 37 States retain nonunified trial court systems featuring a sometimes baffling array of courts of general and limited jurisdiction.

As the June 1999 report of the National Task Force on Court Automation and Integration noted, the organizational and funding structures of State courts are also widely varied. "In some states, all court staff works for a centralized unified State court administrative office. In others, the administrative office plays a very minor role in court operations."[112] The operation of a highly centralized urban court may be significantly different than operations of a small rural court in a State with a decentralized court system. Even in States that have more centralized court systems, not all information is necessarily reported centrally, making it necessary in many cases for a vendor to seek information from numerous local courts. Many commercial vendors offer to conduct criminal background checks at the county level for any county in the country.[113]

Variations in the structure of State court systems can also have an impact on the types of offenses that are considered criminal filings. "For example, criminal filings in Connecticut, Illinois, and Minnesota include ordinance violation cases, which are typically reported in traffic caseloads in other states."[114]

Variations in automation levels also have a dramatic impact on commercial vendors. While the courts have made considerable progress over the past few years in automating their records, not all

---

[105]Florida has made a fiscal decision not to provide a bulk data discount since the State uses the revenue generated by noncriminal justice background checks to pay for the maintenance and operation of its criminal history database and to facilitate access for public safety purposes.

[106]Florida Department of Law Enforcement, "Obtaining Criminal History Information," available at <www.fdle.state.fl.us/criminalhistory/> (visited June 28, 2004). Hereafter, FDLE site. Even without bulk data sales, FDLE conducts more than 1 million checks a year, with commercial vendors being the largest requestor of data. SEARCH, *Report of the National Task Force on Privacy, Technology, and Criminal Justice Information,* Privacy, Technology, and Criminal Justice Information series, NCJ 187669 (Washington, DC: U.S. Department of Justice, Bureau of Justice Statistics, August 2001) at p. 21. Available at <www.ojp.usdoj.gov/bjs/abstract/rntfptcj.htm> (visited June 28, 2004). Hereafter, Privacy Task Force report.

[107]Brian Ostrom, et al, *Examining the Work of State Courts, 2002: A National Perspective from the Court Statistics Project* (Williamsburg, Va.: National Center for State Courts, 2003) at pp. 10, 13.

[108]Ibid., at p. 56.

[109]Ibid., at p. 57.

[110]Brian J. Ostrom and Neal B. Kauder, *Examining the Work of State Courts, 1996: A National Perspective from the Court Statistics Project* (Williamsburg, Va.: National Center for State Courts, 1997) at p. 12.

[111]Ibid.

[112]*Report of the National Task Force on Court Automation and Integration* (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Assistance, 1999) at p. 9 (internal citations omitted). Available at <www.ncjrs.org/pdffiles1/177601.pdf> (visited June 28, 2004).

[113]*See, for example,* NBD Criminal Record Searches, *supra* note 48.

[114]Brian Ostrom, et al., *Examining the Work of State Courts, 2001: A National Perspective from the Court Statistics Project* (Williamsburg, Va.: National Center for State Courts, 2001) at p. 60.

court records have been automated.

Finally, the rules of each court can impact the information available to a commercial vendor and the amount of time and expense that obtaining information from the court entails. In February 2003, the Superior Court of Santa Clara, Calif., for example, ordered, for privacy reasons, that all dates of birth be removed from the publicly available index for criminal records and from all microfiche sets sold to employers and screening companies.[115] As a result, commercial vendors could no longer verify date of birth themselves. Instead, they had to utilize court personnel to do so (and the court limited the number of daily requests for date of birth verification to 25 per company). The policy change was short-lived, however. The court reversed course, amid a flurry of complaints from commercial vendors, and access to date-of-birth data was restored effective March 1, 2003.[116]

2. Corrections departments

While the courts customarily have served as the main source of criminal justice information for commercial vendors, corrections facilities in recent years have become an increasingly major source of data. Court structure and organization vary widely, but State and Federal prison systems are more uniformly (but not universally) centralized, often providing a means of obtaining statewide data from one source. In addition to information on the more than 1.4 million inmates under the jurisdiction of Federal and State adult correctional authorities[117] (who are of little immediate interest to commercial vendors because they are unlikely to be applying for a job, rental housing, etc., while incarcerated), the information systems of corrections departments typically include information about former inmates who have completed their term or have been pardoned or paroled.

The Federal Government and many States make corrections and parole information readily available to the public, including through Internet Web sites. In March 2003, for example, Georgia unveiled an Internet site, nicknamed "Know thy Neighbor," "that allows people to see if parolees live in their neighborhood."[118] The 21,000 parolees in the site's database can be searched by ZIP code, name, or prison identification number. Once an individual's record is found, the site provides the parolee's "picture, home address, physical description, beginning and ending parole date, and most serious offense."[119] The State plans to update the database daily.[120] The sponsor of the legislation that created the site dismissed questions of whether the program constituted an invasion of privacy:

> "Technically, [the parolees] haven't served their time …They're still under state supervision, and if he doesn't want to live under this kind of condition, he can stay in prison."[121]

Today some commercial vendors obtain a significant amount of their criminal justice information, either in terms of number of records or number of jurisdictions, from corrections agencies. According to one Task Force member, for example, while the mix of records constantly changes, at one point his company obtained more than 60% of the criminal justice

[115]BRB Publications, "The Public Record Update, February 2003" (Feb. 2003) available at <www.brbpub.com> (visited June 28, 2004).

[116]Ibid.

[117]Paige M. Harrison and Allen J. Beck, "Prisoners in 2002," *Bulletin* series, NCJ 200248 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, July 2003, rev'd Aug. 27, 2003) at p. 1. The total number of persons incarcerated at the end of 2002 was 2,166,260. Of these, 1,361,258 were under the jurisdiction of Federal and State adult correctional facilities (excluding State and Federal prisoners in local jails). Another 665,475 persons were incarcerated in local jails; 110,284 in juvenile facilities (as of October 2000), and the remainder in territorial prisons, jails in Indian country, Bureau of Immigration and Customs Enforcement (formerly Immigration and Naturalization Service) facilities, and military facilities. Ibid. An additional 753,141 persons were on parole at the end of 2002. Lauren E. Glaze, "Probation and Parole in the United States, 2002," *Bulletin* series, NCJ 201135 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, August 2003) at p. 1.

[118]Jerry Carnes, "Felon Next Door? Check the Web," WXIA TV Atlanta (Mar. 13, 2003) transcript available at <www.11alive.com/news/news_article.asp?storyid=28915> (visited Apr. 5, 2004). Hereafter, Carnes newscast.

[119]Ibid.

[120]"Georgia Online Database Identifies and Traces Parolees," *Government Technology* (Mar. 14, 2003) available at <www.govtech.net/news/news.php?id=43516> (visited Apr. 5, 2004).

[121]Carnes newscast, *supra* note 118, quoting Georgia State senator Eric Johnson (R-Savannah).

information in its databases from corrections sources, compared to 35% from the courts. Similarly, as of January 2004, Rapsheets.com's National Criminal Index contained records from 45 States and the District of Columbia.[122] Corrections department data, without statewide court disposition data, was the source of information for 18 States and the District of Columbia.[123] Court dispositions, with or without sex offender registry data, were the source of information for 7 States, and both corrections and statewide court disposition data were sourced for 13 States.[124] Sex offender registry data was available from 36 States and the District of Columbia (and was the sole source of data in 6 States).[125]

Not surprisingly, information available from corrections departments varies by State. For example:

- Data obtained from State departments of corrections may or may not include information on persons incarcerated in county or municipal jails.
- In some States, corrections data include only information regarding the most serious offense for which the offender was most recently incarcerated because, in the course of designing their systems, some corrections departments determined that this was the only information needed for corrections administration. As a result, information about convictions that gave rise to prior incarcerations or lesser offenses would not be available.
- Corrections data typically report the release date and whether the individual was released on parole, but may not include details about other potential reasons for release, such as an appellate reversal of the individual's conviction.
- Corrections data typically include information only about individuals who actually have come under the supervision of the department of corrections and may not, therefore, include information about individuals who were convicted of a crime, but only placed on probation or some alternative sentence.
- In some cases, it is possible for commercial vendors to obtain information about individuals currently incarcerated, but not historical information. In such cases, some vendors may keep the information on file for future use once the individual has been released.

3. State criminal history repositories

State central repositories—now established in every State—are responsible for the collection, maintenance, and dissemination of criminal history records. The State repositories are agencies or bureaus within State governments, often housed within the State police or a cabinet-level agency with public safety and criminal justice responsibilities.[126] Typically, the repositories are charged under State law with establishing comprehensive files of criminal history records; establishing an efficient and timely system for retrieving the records; ensuring that the records are accurate and up-to-date; and establishing rules and regulations governing the dissemination of records to criminal justice and noncriminal justice users (State and Federal law also establish such standards).[127] In addition, State repositories are often responsible for maintaining fingerprint and other identification records.

The core mission of the repositories is to maintain comprehensive criminal history records, popularly referred to as "rap sheets." Criminal history records typically contain information identifying the subject of the record, including name and numeric identifiers, such as Social Security number, physical characteristics, and fingerprints.[128] Criminal history records also include information about the record subject's current and past involvement with the criminal justice system, including arrests or other formal criminal charges and any dispositions resulting from these arrests or charges.[129] The repositories frequently limit their collection of criminal history information to felonies or serious misdemean-

[122]Rapsheets.com Web site at <www.rapsheets.com/business/aboutdata.asp> (visited Jan. 20, 2004).

[123]Ibid. For some of these States, Rapsheets.com did provide limited non-statewide court data, for example, from only a few counties.

[124]Ibid. In the final State, California, only superior court records from four counties were available. Ibid.

[125]Ibid.

[126]Robert R. Belair and Paul L. Woodard, *Use and Management of Criminal History Record Information: A Comprehensive Report*, NCJ 143501 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, November 1993) at p. 19.

[127]Ibid.

[128]Ibid., at p. 22.

[129]Ibid.

ors.[130] Other types of criminal justice information are seldom included in criminal history files, including "investigative information," "intelligence information," traffic offenses, and certain other petty offenses, all of which are excluded from the definition of "criminal history records" in Federal regulations governing federally funded record systems.[131]

Criminal history information is reported to the State repositories by courts and criminal justice agencies at every level of government and at each stage in the criminal justice process (by police departments, prosecutors' offices, courts, and corrections agencies).[132] Indeed, many State and Federal statutes mandate that courts and criminal justice agencies report information to the central repositories. While the particulars of these requirements vary, they are designed to ensure that record-originating agencies—such as prosecutors, courts, parole, and corrections agencies—provide prompt and accurate data to the State repositories.[133]

Originally, the primary function of the State repositories was to facilitate the maintenance and exchange of criminal history information within the criminal justice community. Over the years, however, noncriminal justice uses, particularly background checks for employment purposes, have steadily and, in many cases, dramatically increased. In some States, noncriminal justice requests now exceed the number of criminal justice requests received each year.[134]

According to the Bureau of Justice Statistics, as of July 2001, State criminal history repositories "held approximately 63.6 million criminal records on individuals. About 9 out of 10 of these records were automated."[135] The number of States that boast 100% automation of their criminal history records has been steadily increasing. As of July 1, 2001, for example, 23 States had fully automated criminal history files, compared to only 18 States in 1995.[136] Another 13 States and the District of Columbia reported that "over 80% of their criminal history records were in automated form as of July 1, 2001." Six States reported less than 60% of their records were automated (figures vary from 28% to 59%).[137] "Of those States that maintain partially automated criminal history files, 22 have a policy to automate the offender's entire record if an offender with a prior manual record is arrested. Four States and the District of Columbia automate only the new information on the record."[138]

State criminal history repositories receive disposition information from a variety of sources and by a variety of methods:[139]

- In 30 States and the District of Columbia, repositories receive final disposition information from law enforcement agencies. Eleven States rely only on the mail to receive these dispositions, while 1 State receives all dispositions electronically from law enforcement agencies.
- In 32 States, repositories receive disposition information from prosecutors. Half of these States receive the disposition information by mail only, 4 States rely solely on electronic transmission, and the remaining 12 States rely on a combination of mail, fax, and electronic transmission.
- In 46 States, repositories receive disposition information from trial courts or the State court administrator's office. In 15 States, this information is received only by mail, while 31 States receive the information electronically.

State law largely regulates noncriminal justice access to information in the State repositories. Repositories in 43 States and territories responded to a March 2001 SEARCH e-mail survey regarding the extent to which they disclose criminal history information to the public (that is, to noncriminal justice users such as employers and vendors).[140] More than two-thirds of the responding repositories reported disclosing at least some criminal history information to the public.

Information disclosed by the State repositories varies widely, depending upon State law. Some States disclose everything on file,

[130]Ibid., at p. 23.

[131]Ibid.

[132]Ibid., at p. 26.

[133]Ibid., at p. 28.

[134]See 68 *Federal Register* 9098 (Feb. 27, 2003).

[135]Bureau of Justice Statistics, "Improving Criminal History Records for Background Checks," *Highlights* series, NCJ 192928 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, Feb. 11, 2002) at p. 1.

[136]Ibid., at p. 4.

[137]Ibid.

[138]Ibid.

[139]Ibid., at p. 5.

[140]SEARCH repository survey, *supra* note 72.

with the exception of sealed or expunged records, while others disclose only adult offender conviction data that is less than 10 years old. Some States require the submission of the subject's fingerprints as a prerequisite for disclosure, while others make information available on the basis of name-plus-identifier checks.

- Of the 29 repositories indicating that "anyone" could obtain criminal history information, 19 limited their disclosure to conviction information or conviction information plus information on pending cases. The remaining 10 States generally provide all information, with the exception of sealed or purged data.
- Fifteen repositories report notifying the individual to whom the records pertain when a noncriminal justice user requests a copy of the record.
- Fees charged by the repositories ranged from $2 to $49, depending upon the requester and whether the check is a name-based check or a fingerprint-based check. In many States, fees are waived or reduced for nonprofit organizations that deal with vulnerable populations such as children, the disabled, and the elderly.[141]

4. Relative "value" of data from repositories, courts, and corrections departments

It is the sense of the Task Force that State repositories represent the best possible single source of State criminal history information for serious offenses ("minor" offenses, particularly those offenses for which fingerprinting is not required, are not customarily reported to State repositories). The State repositories create a central point of contact in a State where various sources of data that may modify existing records can be received and integrated into one record. However, given that repository information is either not always available or not cost-effective, obtaining information directly from the courts and corrections departments is by far the prevalent industry practice.

a. Repository data

The State repository records are not always comprehensive, in some cases by design. State law varies with respect to which offenses local agencies are required to submit to the repository, with minor offenses often omitted. In addition, the State repositories customarily receive only records pertaining to offenses where fingerprinting has occurred. Therefore, even if an offense is otherwise reportable, if police cite and release an individual for an offense, rather than taking the person in for fingerprinting, the offense may not make it to the State repository unless the individual is later fingerprinted. Furthermore, even where reporting to the repository is required, that does not necessarily mean that a local agency complies (or complies expeditiously).

These points were highlighted in a December 2002 technical report from the Defense Personnel Security Research Center (PERSEREC) on the reliability of centralized criminal record repository checks in lieu of local criminal court and justice agency checks (LACs).[142] Given the extensive criminal background checks conducted by the military for security clearances and related purposes, the study was designed to examine "the consistency of information available between local, state, and national repositories" of criminal history record information, presumably to determine whether the military could replace LACs with centralized checks.[143] The report sample comprised four States: California, Florida, Pennsylvania, and Indiana.

The report concluded that "the degree to which evidence of criminal conduct would be lost if centralized repository checks were used in lieu of LACs depended both on the type of criminal conduct and on the agency originating the arrest and/or conviction information."[144] The report found:

- For regularly fingerprinted offenses, the State repositories and the FBI "together identified approximately 70% of offense information found through LACs in California, 89% of the information found through LACs in Florida, and 85% of the offenses identified in Pennsylvania. The Indiana state repository in combination with the [Interstate Identification Index System (III)], however, identified only 32%

[141]Ibid.

[142]Kelly R. Buck and F. Michael Reed, *Reliability of Centralized Criminal Record Repository Checks in Lieu of Local Criminal Justice Agency Checks in Four U.S. States: California, Florida, Pennsylvania, and Indiana* (Monterey, Ca.: Defense Personnel Security Research Center, December 2002). Hereafter, Buck and Reed report.

[143]Ibid., at p. ix.

[144]Ibid.

of the offense information surfaced through LACs in that state."[145]

- "For all types of offenses that can be identified through LACs, the California repository identified 43.3%, the Florida state repository identified 61.2%, and the Pennsylvania state repository identified 41.4%. Only 18.8% of the offense information found through LACs in Indiana could be identified via checks of the Indiana state repository."[146]

With respect to the reliability of LAC reporting, the PERSEREC report recommended that the Defense Department "take into account the reliability of reporting by individual criminal justice agencies to central repositories in any decision to replace all LACs with central state repository checks," suggesting that each agency would need to be evaluated independently to assess the reliability of its reporting to the repository.[147]

Commercial vendors that have found gaps in centralized checks echo these findings. ChoicePoint, for example, reports that it ran parallel criminal background checks for more than 8,000 employees of an airport in Texas. According to ChoicePoint, checks on 186 of these employees returned adverse information that was not returned by checks conducted through the FBI.

[145]Ibid.

[146]Ibid.

[147]Ibid., at p. x.

b. Court and corrections data

Members of the Task Force reported that some vendors have found corrections data to be more accessible for bulk purchase than court data, although it was the sense of the Task Force that court data increasingly are being made more readily available in bulk as courts continue to automate their records.[148] Court data often are viewed as being more complete because the data include cases where the individual did not come under correctional supervision (an important deficiency, given that nearly 4 million people were on probation at the end of 2001).[149] Where a traditional check is being made, court data are more likely to be used (along with repository data, if available).

There are advantages and disadvantages to both statewide corrections searches and county court searches. Corrections department databases "typically include only felons who have been placed under the supervision of the DOC [Department of Corrections]. While they include felons who have been convicted by courts throughout the state, these records typically do not include records of offenders who have been convicted of misdemeanors or first-time felons who have been placed on probation under local supervision… DOC databases usually include information about the current status of offenders following their release from incarceration; for example, their parole status and when they were released from supervision."[150]

"County court records usually include convictions, both misdemeanors and felonies, regardless of the agency that supervises the offender following conviction. However, the county court records do not include any information about the status of the offender following conviction. Of course, county court records include the records for only that county. So if an applicant lives in one county, but commits a crime in another county, a false report will be returned if surrounding counties are not checked."[151]

F. Factors in the growing sale of criminal justice information by commercial vendors

A number of factors are driving the growth of the criminal justice information sector of the commercial information industry. Some of these factors (such as the response to September 11) reflect increased demand for criminal justice information for noncriminal justice purposes, generally, and have increased demands on courts and public agencies as well as the

[148]System limitations have traditionally acted as a type of *de facto* barrier to access to data, particularly with respect to bulk data requests because a court or agency often could decline to furnish the requested information because it lacked the technical capacity to comply with the request. As courts (and agencies) have increasingly automated, however, this barrier is diminished.

[149]Lauren E. Glaze, "Probation and Parole in the United States, 2001," *Bulletin* series, NCJ 195669 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, August 2002) at p. 1.

[150]National Background Data, "Frequently Asked Questions," available at <www.nationalbackgrounddata.com> (visited Jan. 20, 2004).

[151]Ibid.

commercial vendors. Other factors, however, have helped enable the growth of commercial vendors as an alternative to courts and public agencies.

1. Automation of criminal justice records

Automation of court and criminal justice agency systems has been a major factor in the growth of the commercial vendor industry as a way to distribute criminal justice information. While automation started in the late 1960s with the State repositories, in recent years, the courts, as well as corrections departments and other criminal justice agencies, have greatly accelerated their automation efforts. The Federal Government has provided significant funding to assist the States in automating their criminal justice information systems.

Automation has made it significantly faster and easier for commercial vendors to obtain criminal justice information. Where it was once necessary to review paper indexes and updates, it is now often possible to do quick electronic searches, which, because of dial-up access and the Internet, can sometimes be conducted without going to the courthouse.

Automation, coupled with the willingness of most courts and even some agencies to make their automated data available in bulk, has allowed commercial vendors to build private criminal justice information libraries containing millions of criminal justice records. Theoretically, it would be possible to build such libraries using paper records.[152] To do so, however, would consume vastly more manpower and generate vastly greater expense, making the economic viability of such private systems (as opposed to traditional, "as-needed" searches) highly questionable.

2. Technology revolution

a. Computing power

It is difficult to overstate the importance that advances in computing power have played in the growth of the commercial information industry. As the National Task Force on Privacy, Technology, and Criminal Justice Information noted in its report, "[t]echnological advances have made computers smaller, faster, and capable of storing ever-increasing amounts of data in seemingly ever-decreasing amounts of space."[153] In addition, the Privacy Task Force report noted, advances in software and computer programming have supported "the creation of 'data warehouses' where large amounts of information are accumulated and available to be searched on the basis of a multitude of discrete selection criteria."[154]

Advances in computing power and information storage capabilities, coupled with the ability to purchase criminal justice information in bulk from numerous courts and criminal justice agencies, have allowed commercial vendors to create data warehouses that permit their customers to conduct a single search of criminal records that is virtually nationwide in scope. As previously noted, since November 2001, at least three commercial vendors have launched such products.

b. The Internet

As the Privacy Task Force report noted, "perhaps the most important technological development underpinning the need for a reassessment of the privacy landscape [is] the Internet."[155] As with so many other products and services, the Internet provides a convenient, low-cost means of advertising the availability of criminal justice information products to a wide audience, coupled with an inexpensive means of distribution. Criminal justice information can be ordered from home or office with a few lines of data entry and a few clicks of the mouse.

The Internet also can affect the reasons for which criminal justice information is obtained. Those who "need to know" whether an individual has a criminal background are likely to attempt to obtain the information even if it is difficult and expensive to obtain. For those who merely are curious and "want to know," however, the Internet greatly facilitates (and encourages) access to information for which the browser would not be inclined to make a trip to the courthouse.

In addition, when coupled with the automation of criminal justice records and the increasing power and decreasing cost of computers, the Internet creates the potential for small vendors, who would otherwise be unable to hurdle barriers to entry or, at most, would be only local players, instead to become national information providers. Rapsheets.com, for example, which, as previously noted, bills

[152]Acxiom, for example, creates its telephone directory products by hiring people to enter the content of every white pages directory in the United States and Canada.

[153]Privacy Task Force report, *supra* note 106, at p. 41.

[154]Ibid.

[155]Ibid., at p. 48.

itself as having one of the largest criminal justice information databases in the country, with more than 160 million records, had only 9 employees as of May 2002.[156] The Internet also facilitates the development of niche markets. A background company called CheckMate, for instance, caters to singles who want to learn more about their current or prospective dating partners.[157]

Use of the Internet to disseminate criminal justice information is not limited to commercial vendors. In States where it is legally permissible, State repositories, courts, and corrections departments are making criminal justice information available online, either for a fee or at no charge. This trend is occurring despite the fact that in a 2000 opinion survey, sponsored by BJS and SEARCH, 90% of respondents opposed State agencies making criminal justice record information available on the Internet.[158]

Courts, too, are putting more and more records on the Internet. In Oklahoma, for example, the courts put virtually everything online, including nonconviction information, such as newly filed charges.[159] As Oklahoma's courts Web site states:

> Oklahoma has one of the largest initiatives in the nation for providing court docket information on the internet. Unlike most states, Oklahoma is striving to complete a statewide case tracking system and make the information within that system available on a real time basis via the internet. The cost of this service is borne by the judicial system, so there is no cost to the user for obtaining court information from Oklahoma. Currently, information from 9 of the largest counties in Oklahoma, as well as information from every appellate court in Oklahoma, is available via this system. There is no time delay...the information is available as soon as it is entered by the court clerk.[160]

Information from courts in other Oklahoma counties is available through a separate system.[161] These records are not updated in real time, but are kept reasonably current through frequent updates by most courts.

Some State corrections departments, as well as the Federal Bureau of Prisons, also make information publicly available over the Internet. In New York, for example, the State Department of Correctional Services provides an online look-up service that provides "interested parties with information on the status and location of inmates incarcerated in a New York State Department of Correctional Services prison. Information is also provided on former inmates…telling when and why the inmate was released."[162]

The database includes "everyone sentenced to state prison since the early 1970s … except youthful offenders and those who have had their convictions set aside by a court."[163] The database can be searched with as little as a partial last name. Information returned about an offender may include: name; sex; full date of birth; department identification number; incarceration status; facility of incarceration; race/ethnicity; dates of commitment and release; latest release date and type; up to four crimes that resulted in incarceration; aggregate sentence information; and information pertaining to parole eligibility.

The Federal Bureau of Prisons has a similar site, but limits the information disclosed to name, registration number, age, race, sex, projected or actual release date, and location in the Federal prison system.[164] Searches can be conducted by inmate identification number or first and last name.[165] The Arkansas Department of Corrections not only facilitates searches of its inmate database using a variety of search criteria, it

---

[156] Walker article, *supra* note 27.

[157] *See* <www.checkmate1.com/>.

[158] SEARCH, *Public Attitudes Toward Uses of Criminal History Information*, Privacy, Technology, and Criminal Justice Information series, NCJ 187663 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, 2001) at p. 45.

[159] *See* <www.oscn.net/>. Web site visitors may search the daily dockets of State district courts by judge, the type of case before each judge, event, event before each judge, case type, or simply by county.

[160] Oklahoma State Courts Network, "Dockets of Oklahoma Courts," available at <www.oscn.net/applications/oscn/start.asp?viewType=DOCKETS> (visited Jan. 20, 2004).

[161] *See* <www.odcr.com/>.

[162] *See* "Inmate Lookup – General Instructions (Overview)," available at <www.docs.state.ny.us/univinq/fpmsovrv.htm> (visited Jan.20, 2004).

[163] "Who's Listed Here?," at ibid.

[164] Federal Bureau of Prisons, "Inmate Locator," available at <www.bop.gov> (visited Jan. 20, 2004).

[165] Ibid.

permits visitors to download its inmate database free of charge.[166]

In some States, repositories are also making information available online. In Washington, for example, the Washington State Patrol Identification and Criminal History Section has established a Web site "as the official Internet source providing criminal history conviction information for the state of Washington."[167] The database includes "conviction information, arrests less than one year old with dispositions pending, dependency proceedings, and information regarding registered sex and kidnap offenders."[168] Users are charged $10 per search, payable by credit card or pre-established account, and the fee can be waived for certain non-profits for searches of convictions for crimes against children or vulnerable adults.[169] Florida provides another example of repository use of the Internet. In Florida, a name-based check can be ordered online from the repository for $23.[170]

3. The response to September 11

Background checks, of course, have long been used as a tool to screen employees and volunteers for suitability, particularly in cases where the individual would be in a position of trust involving money, secure areas, or vulnerable populations involving children, the disabled, and the elderly. There is reason to believe that criminal background checks were on the increase even before September 11. Surveys by one background screening company, for example, "suggest that 64 percent of U.S. businesses did some type of criminal record check on…employees [in 2000], up from 44 percent in 1998."[171] Similarly, a 2000 survey by the Society for Human Resources Management "found that 61 percent of hiring managers polled had conducted such screenings within the previous year, compared with 44 percent who said they had done a screening regularly in a separate study two years earlier."[172]

Hard industrywide figures are unavailable. It is estimated that new congressional mandates for background checks after September 11 will result in more than a million background checks.[173] In addition to mandates, courts and government agencies are promoting background checks. The Food and Drug Administration, for example, has issued nonbinding "good practice" guidelines recommending that food establishment operators conduct criminal background checks on all employees.[174] In another example, the National Task Force on Court Automation and Integration, in a November 2001 draft report focusing on post-September 11 court system information technology priorities, recommended that the courts "determine the feasibility of courts conducting background checks of all existing and future employees with the rigor accorded background screening of other governmental employees in positions of trust."[175]

Anecdotal evidence suggests a surge in criminal background checks in the immediate aftermath of September 11, even in areas where the government has not newly mandated criminal background checks. The Associated Press reported, for example, that "Two days after terrorist attacks toppled with [sic] the World Trade Center, the chief executive of Empire International spent $40,000 for criminal background checks on all 500 of his livery drivers, most of whom work in New York City. He couldn't really afford it.… But it was the only way he could think of to reassure his clients that they're safe

[166]Arkansas Department of Corrections, "Inmate Population Information Search," available at <www.state.ar.us/doc/inmate_info/> (visited Jan. 20, 2004).

[167]Washington State Patrol, "WSP Watch: Important Introductory Information," available at <https://watch.wsp.wa.gov/> (visited Jan. 20, 2004).

[168] Ibid.

[169] Ibid.

[170]FDLE site, *supra* note 106.

[171]Kim Curtis, "Company Background Checks More Common," Associated Press (Sept. 23, 2001). Hereafter, Curtis article.

[172]Tahmincioglu article, *supra* note 87.

[173]In February 2002, the Airline Pilots Association alone estimated that "up to 1 million aviation employees who have access to secure areas will be fingerprinted, because no screeners had FBI background checks prior to 1998 and no pilots prior to 1996." Ron Scherer, "New step for job applicants: FBI checks," *Christian Science Monitor* (Feb. 1, 2002) available in the archive section at <www.csmonitor.com>.

[174]FDA Guidance, *supra* note 1, recommended that operators have "a criminal background check performed by local law enforcement or by a contract service provider." An earlier version of the guidance issued on Jan. 9, 2002, also recommended checking the FBI Watchlist.

[175]National Task Force on Court Automation and Integration, *Court Systems Information Technology Priorities in the Aftermath of the Events of September 11, 2001* (Sacramento: SEARCH, Nov. 27, 2001 draft) at p. 3.

with his drivers, some of whom have Middle Eastern backgrounds."[176]

Similarly, the "terrorist attacks so unnerved…a senior vice president for the Comforce Corporation…that one week after they occurred he ordered criminal background checks on all information technology employees with jobs in Internet security and networking systems support."[177] The executive is quoted as saying that while it was unlikely the company had hired terrorists: "We want to make sure someone with a felony history hasn't snuck into our organization."[178]

A March 2002 survey by Building Owner and Managers Association (BOMA) International and the Urban Land Institute of 200 of their members found that 60.9% of commercial property owners and managers conducted employee background checks on their employees prior to September 11, 2001; after September 11, the figure rose to 66.8%.[179]

Immediately after September 11, ChoicePoint reported a "dramatic increase" in inquiries and a 30% increase in business from security firms. According to security firm Kroll, Inc., the number of background checks it conducted increased 20% from 2001 to 2002.[180] HireCheck, another commercial vendor, reported a 25% increase in business.[181] "Employee screening companies are seeing an unexpected rise in business despite a decline in hiring. That's because the scope of checks on new hires has widened and current employees also get checks."[182] Or in some cases, current employees got rechecked. "Mark Black, supervisor of investigations for the Anne Arundel County Public Schools in Annapolis, Md., for example, decided to recheck the backgrounds of 200 bus drivers who had access to a military installation where some students live. While all drivers had undergone criminal screenings before, he said, 'given everything that's going on, we wanted to make sure.' "[183]

There are a variety of potential explanations for the increase in background checking activity. The examples cited above suggest an abundance of caution and a desire to do something to reassure clients as reasons for the increase. An informal survey by HireCheck found that about one-half of the orders they received in the aftermath of September 11 were following standard procedures and the other half were increasing their background checking.[184] These customers "were not expecting to uncover a terrorist, but most, especially those in transportation, said they wanted to provide an extra level of security to their clients."[185]

The growing emphasis on security also has led corporate employers to reassess their processes for vetting prospective employees, including background checks. Some businesses, for example, "increased the number of job categories for which they conducted investigations and the types of searches being conducted."[186] In addition, "businesses have expanded their criminal history search area. In the past, many employers would search only the current county or state of residence. Today, companies automatically research prior residences, in most cases for a seven-year period."[187]

Verizon Communications, for example, put a much-enhanced background screening protocol into effect in February 2002.[188] The new protocol: expanded the timeframe reviewed during a background investigation from 5

[176]Curtis article, *supra* note 171.

[177]Tahmincioglu article, *supra* note 87.

[178]Ibid.

[179]BOMA International, "National Survey of Security Concerns Within the Real Estate Industry" (undated) at pp. 2, 6. Available at <www.boma.org/ProductsAndResearch/SafetyAndEmergencyPlanning/natsurveysecconcerns.htm> (visited June 28, 2004). Hereafter, BOMA survey.

[180]Ann Davis, "Firms Dig Deep Into Workers' Pasts Amid Post-Sept. 11 Security Anxiety," *Wall Street Journal* (Classroom Edition) (Mar. 12, 2002). Hereafter, Davis article.

[181]Tahmincioglu article, *supra* note 87.

[182]Aja Whitaker, "Employee screening rises while hiring remains low," *The* [Tampa Bay, Fla.] *Business Journal* (Jan. 18, 2002) available at <www.tampabay.bizjournals.com>.

[183]Tahmincioglu article, *supra* note 87.

[184]Ibid.

[185]Ibid (quoting Renee Svec of Hirecheck Inc.).

[186] Society for Human Resources Management, "Life goes on: the Sept. 11 attacks were over within hours, but the effects linger even today. This is how employers are adapting," *HR Magazine* (Vol. 47: Issue 9, Sept. 1, 2002) (quoting Jackie Kohn, Graymark Security Group).

[187]Ibid.

[188]Ibid (comments of Barbara Walker, Executive Director of Human Resources Communications and Research, Verizon Communications, Dallas).

to 7 years; expanded the criminal background check to include a national check; and added an international component for foreign new hires with certain visas.[189] Where the foreign employee has been in the United States for fewer than 7 years, the company is now conducting an international background check in the new employee's country of origin or residence.[190]

One area where organizations appear to be focusing additional scrutiny is on the organization's service providers and contract workers. According to a March 2002 survey, for example, the "single security upgrade most frequently utilized following September 11 [by commercial building managers] was tighter vendor security, which included requirements for vendor identification, vendor check-in and requests for vendors to conduct employee background checks."[191] The National Basketball Association required food and merchandise vendors for the 2002 All Star game to submit the names of employees in advance so that criminal background checks could be conducted.[192] Pharmaceutical giant Eli Lilly received considerable media attention when it barred numerous contract workers from Lilly facilities following criminal background checks (many of whom lost their jobs as a result).[193] In another example, two major movie studios retained a security firm, Kroll Inc., to confirm that tens of thousands of outside vendors (caterers, mechanics, medics, etc.) do not have criminal histories.[194]

Another anecdotal reason for increased background checks in the aftermath of September 11 is that companies that had been lax in meeting pre-existing background check obligations have since tightened their practices. As an October 2001 *New York Times* article noted, "At the Chico [Calif.] Municipal Airport, for example, all employees of airport tenants must undergo criminal background checks before they are allowed in secure areas. Robert Grierson, the airport's manager, said he and his staff have been calling tenants since the [September 11] attacks to remind them of that requirement. 'Sometimes it gets quiet on the other end of the phone,' he said."[195]

4. Marketplace demands

Another factor promoting growth in the commercial vendor market is the ability of commercial vendors to provide additional data and services that are essentially unavailable from courts and criminal justice agencies.

- **One-stop shopping.** Commercial vendors can combine criminal justice information from one State with criminal justice information from another State or combine criminal justice information with other information products that are valued by end-users.
    - In the employment context, this may include the provision of information such as credit reports, driving history information, reference checks, civil litigation information, and verification of Social Security numbers. Some employment screening companies also offer drug-testing services in addition to their information products.
    - Commercial vendors that provide tenant-screening services may supplement criminal justice information with other types of information, including eviction data, credit histories, returned check histories, and rental histories.[196]
    - Commercial vendors that provide background checks to singles seeking more information about prospective dates or spouses supplement criminal justice information with everything from identity-verification services, to checks of marital and divorce records, to asset verification.
    - Because the United States is a highly mobile society, an individual could have criminal justice records in multiple States. It may be more convenient and cost-effective to go to one commercial vendor to obtain information from these various States as opposed to going to the State criminal history repositories, courts, or other agencies in each individual State.

[189] Ibid.

[190] Ibid.

[191] BOMA survey, *supra* note 179, at p. 2.

[192] Davis article, *supra* note 180.

[193] *See, for example,* ibid.

[194] Ibid.

[195] Tahmincioglu article, *supra* note 87.

[196] Ibid.

- **Screening out "irrelevant" or legally impermissible information.** In some States, system design limitations or legal impediments prevent courts or government agencies from providing customized criminal background reports or even from inquiring as to the purpose behind a record request.[197] End-users, however, do not necessarily want to receive everything, particularly information that the end-user is legally prohibited from considering as decisionmaking criteria. Commercial vendors can and do provide this screening function, thereby giving added value to the end-user.

- **Interpreting or packaging the results of the check.** Another way in which commercial vendors may add value for end-users is to assist them in evaluating the results.

  ChoicePoint, for example, offers its tenant screening customers what it refers to as "rules-based decisioning," solutions that recommend rental actions based upon criteria (which may include criminal justice information), established in conjunction with the landlord. The landlord is provided with a recommendation of "Accept with Normal Security Deposit," "Accept with Additional Security Deposit or Guarantor," or "Decline Applicant," along with the reasons for the recommendation.[198]

  Similarly, the Federal Office of Personnel Management—which provides Federal agencies with many services similar to those offered by commercial vendors—provides all information that it obtains as a part of a government background investigation, but screens and scores the data to help the agency reach a decision.

- **Follow-up inquiries.** It is the custom of courts and criminal justice agencies to simply provide the information they have on file at the time it is requested. That information, however, may in some cases be missing dispositions or other data that may not be apparent to an end-user. Commercial vendors, particularly where a traditional, "upon request" report is being prepared, can serve as a useful intermediary, reviewing the information for completeness and taking follow-up steps, such as going to local courts to obtain missing dispositions.

- **Records not sent to repositories.** Information about all offenses is not sent to State repositories. Most repositories, for example, do not accept information on lesser offenses for which the accused is not fingerprinted. Commercial vendors can, however, include such information in their reports by obtaining it from the courts. Examples of information of this type, which varies by State, might include gross misdemeanors, traffic violations, and bounced checks.

- **Capacity.** Capacity limitations, which can limit the speed with which State repositories or courts respond to noncriminal justice requests, can lead some end-users to use commercial vendors instead.[199] Some end-users place a premium on being able to obtain almost instant results on demand. An executive with a temporary staffing company, for example, emphasized the need for being able to conduct speedy background checks in a business where staff is often needed with little prior notice (and the company finds prescreening not to be cost-effective). "The problem is that it takes anywhere from four to six hours on a good day to get the answer back … sometimes it can take as long as 24 hours." "The ability to get online and check [backgrounds] immediately is why we went [with online background checks]."[200]

[197]This is not true in all States, however. In some States, such as California, where legislatures have been very specific about whether a particular offense may or may not be considered for employment or other purposes, State repositories have developed software that modifies the criminal history report to be provided to reflect State law restrictions.

[198]ChoicePoint Inc., "Services," available at <www.residentdata.com> (visited June 28, 2004).

[199]As noted previously, the National Crime Prevention and Privacy Compact Council has recognized that the repositories, particularly post-September 11, lack sufficient capacity to meet the demand for background checks and announced its intention to issue a rule permitting outsourcing certain tasks in order to enhance the capacity of the repositories. *See* 68 *Federal Register* 9098 (Feb. 27, 2003). Of course, capacity can also be a differentiating factor between commercial vendors.

[200]Security Management Online, "Background Checking Moves to the Forefront" (September 2002) available at <www.securitymanagement.com /library/001307.html> (quoting Gary

5. Risk/loss mitigation

Another factor driving the demand for background checks—whether from commercial vendors, courts, or criminal justice agencies—is a desire to mitigate the risk of loss. According to a 2002 University of Florida survey, the average dollar loss per employee theft incident totaled $1,341.02.[201] Many businesses, for example, use background checks in an effort to reduce employee theft by screening out bad employees before they are hired. In the Florida survey, nearly 84 percent of retailers reported using criminal conviction checks as a means of controlling employee theft.[202] Thirty-one percent of respondents anticipated increasing their use of background checks.[203]

Even in cases where employee theft is not an issue, to the extent that recidivism or other factors could lead to turnover of employees with criminal records, employers may be concerned about the costs of training employees who may or may not work out.[204]

The desire to avert risk of loss also extends to efforts to minimize potential legal liability arising from the doctrine of negligent hiring and retention. These doctrines increase demand for criminal background checks because many employers fear that failure to conduct such a check may result in substantial damage awards if the employee later engages in a bad act.[205]

6. Legal framework/ authorization provided by the Fair Credit Reporting Act and State Law

Growth in the commercial information market is also fostered by the Federal Fair Credit Reporting Act (FCRA) and similar State laws (also discussed in more detail in part II). The FCRA and similar State laws implicitly authorize commercial vendors to collect, maintain, and disclose information about consumers, including criminal justice information, for certain statutorily recognized purposes, including employment. Importantly, the FCRA also provides qualified immunity for covered commercial vendors (referred to as "consumer reporting agencies" in the FCRA) and end-users from potential invasion of privacy, defamation, and negligence claims if the information is contained in an FCRA-covered report.[206]

7. Unavailability of State and Federal checks in some jurisdictions

Another factor that contributes to the growth of the commercial information industry's distribution of criminal justice information is that this information may not always be available to employers (and others) through the FBI and central State repositories. Legal access restrictions in many States mean that many end-users are not authorized to obtain criminal justice information from the FBI and State criminal history repositories or may authorize access for only specific purposes. Even where State law provides a basis for obtaining criminal history information, this access may be impractical for the end-user because of fingerprint requirements.

These restrictions result in an unmet demand for criminal background checks. Commercial vendors have been able to fill this demand by bypassing State criminal history repositories and, instead, obtaining the criminal justice information from the courts, corrections departments, and other agencies where public access is not prohibited by law. In addition, given that State repositories customarily do not actively "market" the information products that they may make available to noncriminal justice users under State law, report requestors may not even realize that the State repositories could serve as an alternative to obtaining reports from commercial vendors.

Glaser, regional vice president for Tandem Staffing Solutions in Memphis, Tenn.) (visited June 28, 2004).

[201]Richard C. Hollinger and Jason L. Davis, *2002 National Retail Security Survey Final Report* (Gainesville, Fla.: University of Florida Security Research Project, 2003) at p. 19. Available at <http://web.soc.ufl.edu/SRP/final report_2002.pdf> (visited June 28, 2004). Hereafter, Hollinger Retail report.

[202]Ibid., at p. 13. According to the survey, criminal conviction checks were significantly more likely to be conducted for nonprofessionals, both managers and nonmanagers (78.8%), than for professionals (18.6%).

[203]Ibid.

[204]For a discussion of recidivism rates and the timing of recidivist events in relation to release or parole, please see part III of this report.

[205]For a discussion of the law of negligent hiring, please see part II of this report.

[206]15 U.S.C. § 1681h(e).

Access to FBI and State repository records often is perceived to be the most desirable means to conduct a background check, even if reports from commercial vendors are faster and more easily tailored to the end-user's needs. The National Apartment Association (NAA) and the National Multi Housing Council (NMHC), for example, included increased access to FBI and repository records among their joint Federal legislative priorities for 2003. In providing background for their position, NAA and NMHC note: "In practice, private-sector criminal history databases provide substantial criminal history information much more quickly and flexibly than the [limited existing access to the Interstate Identification Index]. Broader access [to FBI and repository data]…would reduce the possibility of rental housing providers admitting renters whose criminal history is well-known to the federal government."[207]

8. The "bandwagon" effect

Finally, it was the sense of the Task Force that, while difficult to document, the growth in background checks is being driven, at least to some extent, by a "bandwagon" effect, whereby employers, landlords, and others perceive that "everyone else" is conducting criminal background checks and that they will somehow be at a disadvantage or failing to "do their part" to make to make their community a safer place by not conducting some form of a criminal background check.

[207]National Apartment Association and the National Multi Housing Council Joint Legislative Program, *2003 Legislative and Regulatory Priorities* (Washington, D.C.: February 2003). Hereafter, NAA/NMHC Joint Legislative Program.

Part II. Regulation of access to and use of criminal justice record information

Federal and State law, and related regulations, policies, and practices, have a significant impact on—

- the manner in which commercial vendors and end-users obtain and maintain criminal justice record information
- the ability of end-users to use those reports for employment and other purposes
- the safeguards that must be employed to protect the privacy of individuals to whom the information pertains.

With some overlap, these laws, regulations, policies, and practices fall into four broad categories:

1. those that promote, restrict, or otherwise regulate access to criminal justice record information held by governmental sources
2. those that primarily regulate the practices of commercial vendors, such as the Fair Credit Reporting Act
3. those that regulate the information that end-users, particularly employers and landlords, can use to make employment and housing decisions
4. negligence doctrines that promote efforts by employers and landlords to obtain criminal justice record information.

In addition, some commercial vendors have undertaken self-regulatory efforts to govern their information practices.

A. Regulation of access to criminal justice record information held by governmental sources

The first category of relevant legal regulation promotes, restricts, or otherwise regulates access to criminal justice record information held by governmental sources such as the FBI, State criminal history repositories, the courts, and corrections departments.

1. State repositories and the FBI

The laws, regulations, policies, and practices that regulate access to information held by governmental sources fall into two general categories: (1) those that regulate or restrict access to criminal justice record information, and (2) those that authorize or require the conduct of criminal background checks for certain types of employment, such as government employees, airport workers, and workers and volunteers who come into contact with vulnerable populations such as children, the disabled, and the elderly.

We begin by discussing laws and regulations, in both categories, that address criminal history information held by the FBI and State repositories.

a. Federal criminal history record legislation and regulation

Beginning in the late 1960s and extending throughout the 1970s, information privacy standards for criminal justice information and, in particular, criminal history records, received considerable attention in statutory provisions and U.S. Department of Justice (DOJ) regulations. Although the privacy protections that emerged from that debate were not driven by constitutional requirements, constitutional values—such as the presumption that an individual is innocent until proven guilty—have played a role in the development of the law and regulations governing the management of criminal history information.

In 1967, the Report of the President's Commission on Law Enforcement and the Administration of Justice identified the need for an "integrated national information system" and recommended the establishment of a "national law enforcement directory that records an individual's arrests for serious crimes, the disposition of each case, and all subsequent formal contacts with criminal justice agencies related to those arrests." The report also emphasized that it is "essential" to identify and protect security and privacy rights to ensure a fair, credible, and politically acceptable national criminal justice information system.[208] For

[208]Project SEARCH, *Technical Report No. 2: Security and Privacy Considerations in Criminal History Information Systems* (Sacramento: California Crime Technological Research Foundation, 1970) pp. 3–5

most of the last 30 years, the U.S. DOJ, working through the FBI; the Law Enforcement Assistance Administration (LEAA) and its successor agencies, the Office of Justice Programs (OJP), the Bureau of Justice Statistics (BJS), and the Bureau of Justice Assistance (BJA); and the State and local criminal justice information community, including SEARCH and the FBI Criminal Justice Information Services Division's Advisory Policy Board (CJIS APB), have worked toward the implementation of an automated national system for the exchange of criminal history records, along with a set of comprehensive privacy standards.[209]

In 1972, Congress authorized the FBI to "exchange identification records" with State and local officials for "purposes of employment and licensing," provided that the exchange of information is authorized by State statute and approved by the Attorney General, and provided that the exchange of information is made only for official use and is subject to the same restrictions with respect to dissemination as would apply to the FBI.[210]

In 1973, Congress enacted the "Kennedy Amendment" to the Omnibus Crime Control and Safe Streets Act of 1968, which provides that all the criminal history record information collected, maintained, or disseminated by State and local criminal justice agencies with financial support under the Omnibus Crime Control and Safe Streets Act must be made available for review and challenge by record subjects and must be used only for law enforcement and other lawful purposes.[211] Subsequently, DOJ published comprehensive regulations "to assure that criminal history record information…is collected, stored, and disseminated in a manner to ensure the accuracy, completeness, currency, integrity, and security of such information and to protect individual privacy."[212]

The regulations in 28 CFR Part 20 set standards for data quality that are detailed and ambitious. Thus, for example, the regulations require that States maintain accurate records containing no erroneous information and "complete records," defined as containing "information of any dispositions occurring within the State within 90 days after disposition has occurred."[213] The regulations recognize that incomplete or inaccurate criminal history data, particularly arrest information without corresponding disposition information, could have negative implications for the record subject and his or her participation in society.[214]

The regulations give States the discretion to set their own standards for dissemination of criminal history information, but they provide that use of such information shall be limited to the purpose for which it is given.[215] In recognition of the fact that many jurisdictions' conviction data have historically been made available without limitation, the regulations provide that conviction data can be disseminated without specific authorizing legislation.[216] They also provide, however, that the regulations cannot be construed to

(quoting from the President's Commission Report).

[209]Pub. L. No. 92-544, Title II, § 201, 86 Stat. 1115. Privacy Task Force report, *supra* note 106, at p. 17. 28 U.S.C. § 534 provides the statutory authority for the FBI to maintain and disseminate criminal history records, by authorizing the Attorney General to "acquire, collect, classify and preserve criminal identification, crime and other records," and to "exchange such records and information with and for the official use of, authorized officials of the federal government, the States, cities and penal and other institutions."

[210]Pub. L. No. 92-544, Title II, § 201, 86 Stat. 1115. *See* Privacy Task Force report at p. 17.

[211]42 U.S.C. § 3789G(b), as amended by § 524(b) of the Crime Control Act of 1973, Pub. L. No. 93-83 (1973). *See* Privacy Task Force report at p. 17.

[212]28 C.F.R. § 20.01. In developing the regulations, the LEAA was influenced by the recommendations in SEARCH's *Technical Report No. 13,* which was the organization's first comprehensive statement of 25 recommendations for safeguarding the security and privacy of criminal justice information. See *Technical Report No. 13: Standards for the Security and Privacy of Criminal Justice Information* (Sacramento: SEARCH Group, Inc., 1975). Indeed, the Appendix to the regulations refers States to the SEARCH report for guidance in formulating their State plans. 28 C.F.R. Part 20, Appendix § 20.22(a).

[213]28 C.F.R. § 20.21(a). To accomplish the goal of maintaining accurate records, States are required to "institute a process of data collection, entry, storage, and systematic audit that will minimize the possibility of recording and storing inaccurate information," and if inaccurate information of a material nature is found, the State must notify all criminal justice agencies known to have received the inaccurate information. 28 C.F.R at § 20.21(a)(2).

[214]*See, for example,* 28 C.F.R. Part 20, Appendix.

[215]*See* 28 C.F.R. § 20.21(c).

[216]28 C.F.R. § 20.21(b).

negate any State law that limits the dissemination of conviction data.[217] On the other hand, the regulations make a clear distinction between dissemination of conviction data and nonconviction data, which is defined to include arrests more than 1 year old without a disposition and arrests with dispositions favorable to the accused.[218] Under the regulations, nonconviction data cannot be disseminated unless authorized by a State statute, ordinance, executive order, or court rule, decision, or order.[219]

b. National Crime Prevention and Privacy Compact

In October 1998, the Congress enacted the Crime Identification Technology Act,[220] which includes as Title II, the National Crime Prevention and Privacy Compact Act.[221] The National Crime Prevention and Privacy Compact is an interstate and Federal/State compact that is designed to facilitate and regulate the exchange of criminal history information, for noncriminal justice purposes, among the States and the Federal Government. As of January 2004, the Federal Government and 21 States had ratified the Compact, which became effective on April 28, 1999, following its ratification by two States.[222]

The Compact addresses the use, for noncriminal justice purposes, of the Interstate Identification Index system (III), which consists of an index, maintained by the FBI, of all individuals with State or Federal criminal history records, supported by a National Fingerprint File.[223] In enacting the Compact, Congress recognized that the legally authorized noncriminal justice purposes for which criminal history records are exchanged, and the procedures for such exchanges, vary widely from State to State. Congress found that an interstate and Federal/State compact was necessary to facilitate authorized interstate criminal history record exchanges for noncriminal justice purposes on a uniform basis, while permitting each State to effectuate its own dissemination policy within its own borders.[224] The Compact is designed to provide expeditious access to records "in accordance with pertinent Federal and State law," while "simultaneously enhancing the accuracy of the records and safeguarding the information contained therein from unauthorized disclosure or use."[225]

Under the Compact, the FBI and the participating States agree to maintain detailed databases of their criminal history records, including arrests and dispositions; to make them available to each other for noncriminal justice purposes; and to adhere to rules, procedures, and standards established by the Compact Council concerning record dissemination and use, response times, system security, data quality, and other established standards that enhance the accuracy and privacy of the records.[226] The Compact expressly excludes, from the criminal history records subject to the Compact, identification information (such as fingerprint records), if such information does not indicate involvement of the individual with the criminal justice system.[227]

c. State statutes governing the receipt and maintenance of criminal history record information by State repositories

The information that a State repository receives from local agencies and maintains is a function of State law. The offenses for which information is reported to the repositories vary by State. A Defense Personnel Security Research Center technical report illustrated this point through a comparison of what constitutes a reportable offense in California, Florida, Pennsylvania, and Indiana. The report found that fewer offenses are reportable in Pennsylvania and Indi-

---

[217] 28 C.F.R. Part 20, Appendix § 20.21(b).

[218] 28 C.F.R. at § 20.3(q).

[219] 28 C.F.R. at § 20.21(b).

[220] 42 U.S.C. § 14601.

[221] 42 U.S.C. § 14611 et seq.

[222] The States that had ratified the Compact as of December 2003 are: Montana, Georgia, Nevada, Florida, Colorado, Iowa, Connecticut, South Carolina, Arkansas, Kansas, Alaska, Ohio, Oklahoma, Maine, New Jersey, Minnesota, Arizona, Tennessee, North Carolina, New Hampshire, and Missouri. It is expected that most States will ratify in 2–5 years. *See* "National Crime Prevention and Privacy Compact," available at <www.search.org/policy/compact/privacy.asp> (visited June 28, 2004).

[223] The Compact defines "noncriminal justice purposes" to mean purposes authorized by Federal or State law other than those relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances. 42 U.S.C. § 14616, Article I (18).

[224] 42 U.S.C. § 14611(3) and (4).

[225] Ibid., at § 14611(5).

[226] Ibid., at § 14616(b) and Article II. The Compact Council is comprised of State and Federal officials.

[227] Ibid., at Article I (4).

ana than in California and Florida, as the following State highlights demonstrate.[228]

California includes as a reportable offense—

- every arrest and disposition except as otherwise provided by law or as prescribed by the Department of Justice
- any crime or attempted crime that is motivated by ethnicity, gender, sexual orientation, or any disability
- forgery, fraud-bunco, bombings, receiving or selling stolen property, safe and commercial burglary, grand theft, child abuse, homicide, threats, and offenses involving lost, stolen, found, pledged, or pawned property
- DUI (starting in 2000).[229]

Florida includes as a reportable offense—

- all adult felony arrests and, unless specified otherwise by statute, all adult misdemeanor arrests
- any juvenile arrest that would be considered a felony if committed by an adult.

Pennsylvania includes as a reportable offense—

- all felony and misdemeanor offenses
- those summary offenses that become misdemeanor upon a second offense.[230]

Indiana includes as a reportable offense—

- all felonies and certain Class A misdemeanors that the repository superintendent may designate.[231]

While there are variations between States, it is important to note that felonies and at least some misdemeanors are virtually always reportable to the repositories.

d. State statutes governing dissemination of criminal justice record information by State repositories

The bulk of the criminal justice information maintained in the United States is held at the State level; therefore, most of the legislation governing the dissemination and use of this information is found at the State level (with a few important exceptions, discussed elsewhere in this report). Throughout the 1970s and into the 1980s, States adopted statutes based largely on the recommendations of the U.S. DOJ and SEARCH. By the early 1990s, approximately one-half of the States had enacted comprehensive criminal history record legislation, and every State had enacted statutes that address at least some aspects of criminal history records.[232]

Today, while all States tend to adhere to several fundamental principles in protecting the privacy of criminal history record information, State laws establishing the practices and procedures for the dissemination of criminal history information by the State repositories vary widely, ranging from open record States, which permit anyone to obtain access to all but sealed or expunged records, to States that closely regulate disclosure. Summarized below are the governing principles that characterize the general approach taken by most States, and then, by way of example, we discuss with more specificity the application of those principles in the laws of three States.

In general, all States give record subjects the right to inspect their own criminal history records, and most permit the subjects to challenge and/or offer corrections to the information in their records. In addition, most States have formal or informal restrictions that segregate criminal history record information from other types of personal information. Thus, for example, criminal history record information customarily does not include investigative or intelligence information, or medical, employment, financial, or military information.[233]

The States have also adopted standards for ensuring the accuracy and completeness of criminal history record information. For example, the criminal history records maintained in virtually every State repository must be supported by a fingerprint record and, with certain exceptions, requests must be accompanied by a fingerprint. Fingerprint support ensures that the record maintained at the repository related to the correct person, and that the reposi-

[228] Buck and Reed report, *supra* note 142, at pp. 10–11.

[229] California excludes public intoxication offenses unless there is a special justification for reporting them.

[230] "Summary offenses" is a special class of offenses in Pennsylvania, which overlap with misdemeanors in California, Florida, and Indiana.

[231] Buck and Reed report, *supra* note 142, p. 11, Figure 2.

[232] Privacy Task Force report, *supra* note 106, at p. 18.

[233] Ibid., at p. 19.

tory's response similarly related to the correct person.[234] Most States also have laws that permit the purging of nonconviction information; many have adopted standards for the purging of certain conviction information if certain conditions are met; many States also have laws and regulations permitting and otherwise governing the sealing of nonconviction and conviction information. All States have adopted some kind of standards for the security of their repositories, although the nature and extent of the standards vary substantially.[235]

Similarly, all States have adopted laws or regulations setting standards for the use and/or dissemination of criminal history record information. While the standards vary, as a practical matter, every State makes all criminal history record information available for criminal justice purposes, unless the information has been sealed by statute or by court order. Outside of the criminal justice system, conviction information is widely available but nonconviction information may be more difficult to obtain or may be readily available only to certain types of users, such as licensing boards and certain types of employers who employ individuals in highly sensitive positions, such as school bus drivers or childcare workers. In most States, authorized noncriminal justice requestors receive less than the full record; most often they are provided conviction-only information. Except in a few "open record" States such as Florida and Wisconsin, the general public is restricted in its ability to obtain criminal history record information from the central State repositories, except for certain classes of information, such as sex offender registry information.[236] For illustrative purposes, the criminal history record information that is available in each of three States, Florida, Washington, and Massachusetts, is described below. Each of them typifies one of three levels of openness that can be used to characterize the laws of all 50 States.

— Access to criminal justice record information in an "open records" State, such as Florida

In 1977, the Florida Department of Law Enforcement (FDLE) adopted a policy of making all State-generated criminal history records available upon request by any member of the public for any purpose, upon payment of the applicable fees, which are designed to offset the costs of public record access requests.[237] The policy is designed to implement the State's public record law.[238]

In general, requests for criminal history records by noncriminal justice users in Florida fall into two broad categories. The first category is comprised of agencies and organizations with approved statutory authorizations to receive information from the FBI as well as FDLE. State departments and agencies authorized to access information for employment background checks make up the bulk of this category, but it also includes licensing bureaus, universities, State commissions, and the agency responsible for running the State lottery.

The second category comprises agencies and organizations without statutory authorization that are eligible to receive information only from FDLE files, pursuant to the public records law. Requestors in this category may request a search of Florida-generated crimi-

[234]The principal exception for law enforcement occurs in instances where the law enforcement agency does not have the individual in custody and, therefore, cannot provide a fingerprint, or in situations requiring a quick turnaround. In such instances, a name-plus-identifier check is permitted. Ibid., at p. 19.

[235]Ibid., at pp. 19–20.

[236]Ibid., at p. 20. As of 2001, four States were "open records" States: Florida, Wisconsin, Oklahoma, and Iowa. Robert R. Belair, et al., *Use and Management of Criminal History Record Information: A Comprehensive Report, 2001 Update*, Criminal Justice Information Policy series, NCJ 187670 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, December 2001) at p. 52. Hereafter, 2001 Use and Management report.

[237]This section is excerpted from a discussion in the Privacy Task Force report, *supra* 106, at pp. 21–22, which in turn, was based upon information from the FDLE, and Paul L. Woodard, *A Florida Case Study: Availability of Criminal History Records, the Effect of an Open Records Policy* (Sacramento: SEARCH Group, Inc., 1990). Hereafter, Woodard report.

[238]The policy is interpreted in conjunction with Chapter 943 of the Florida Statutes, which regulates the collection, maintenance, and dissemination of criminal justice information. Section 943.053(2) effectively restricts the applicability of the State public records law to Florida-generated records by providing that criminal justice information obtained from the Federal government and other States shall be disseminated only in accordance with Federal law and policy, and the law and policy of the originating State. Similarly, section 943.054(1) restricts the ability of FDLE to make available any information derived from a system of the U.S. DOJ to only those noncriminal justice purposes approved by the Attorney General or the Attorney General's designee. Woodard report, ibid.

nal records for any purpose by paying the appropriate fee. These inquiries are typically "name only," although fingerprints will be compared if supplied by the requestor. Responses to these requests include all unsealed, Florida-generated criminal history records in the FDLE computerized files. According to FDLE officials, while requests are filed by all types of agencies for a wide variety of purposes, the most common reason is employment screening, and most of these requesters are regular users with assigned account numbers to facilitate billing and processing. In addition to requests for an individual's entire criminal history record, FDLE also administers databases of sexual offenders and sexual predators (as defined under Florida law) that the public can search over the Internet.

— Access to criminal justice record information in an "intermediate records" State, such as Washington

In Washington, certified criminal justice agencies may request and receive criminal history record information without restriction for criminal justice purposes. Noncriminal justice entities and individuals may receive access only to conviction information.[239]

The Washington State Patrol (WSP) is responsible for maintaining the Washington repository of criminal history record information. Depending upon the purpose of the request, WSP may respond under two different statutes, the Criminal Records Privacy Act[240] or the Child and Adult Abuse Information Act.[241] Both name and descriptor searches and fingerprint-supported searches are performed.

Requests made pursuant to the Criminal Records Privacy Act—which provide the requestor with conviction information—can be made by anyone for any purpose, without the consent of the record subject. If there is a record, the requestor will receive a report detailing all State of Washington convictions and pending arrests less than 1 year old without disposition, and whether the individual is a registered sex offender or kidnapper. Secondary disclosure of criminal history record information obtained pursuant to this statute is restricted.

Access to criminal history records information pursuant to the Child and Adult Abuse Information Act is limited to "businesses or organizations licensed in the State of Washington; any agency of the State; or other governmental entities that educate, train, treat, supervise, house, or provide recreation to developmentally disabled persons, vulnerable adults, or children under 16 years of age." If a record exists, it will include Washington convictions and pending arrest offenses under 1 year old of "crimes against children or other persons, crimes of financial exploitation, civil adjudications, and sex offender and kidnapper registration information." Requestors are required to provide a copy of the report to the record subject, and further dissemination or use of the record is prohibited. Furthermore, employers who obtain records pursuant to this Act may use them only to make the initial employment decision. Violators are subject to civil damages.

WSP does not make sex offender information publicly available over the Internet, but some sex offender information is available for certain employment background checks. In addition, WSP disseminates limited information on sex offenders to the general public in response to written requests. Some local departments make sex offender information publicly available over the Internet. In addition, and based upon the risk level of the offender, local law enforcement may notify neighbors and community members.

— Access to criminal justice record information in a "closed records" State, such as Massachusetts

The Massachusetts Criminal History Systems Board (CHSB) was created in 1972 and is governed by a 17-member board comprised of representatives from the criminal justice community. The Board handles criminal justice requests for criminal history records electronically; public access requests, which are restricted, are processed using the U.S. mail and e-mail.[242]

[239]This section is excerpted from a discussion in the Privacy Task Force report, *supra* note 106, at pp. 23–24, which, in turn, was based upon information from the Washington State Patrol and Devon B. Adams, *Update 1999: Summary of State Sex Offender Registry Dissemination Procedures*, *Fact Sheet* series, NCJ 177620 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, August 1999) p. 7.

[240]Chapter 10.97 revised Code of Washington (RCW).

[241]RCW §§ 43.43.830-845.

[242]This section is excerpted from a discussion in the Privacy Task Force report, *supra* note 106, at pp. 25–26, which, in turn, was based upon infor-

Public access requests must include the name and date of birth of the subject of the inquiry. Not all criminal history records are available to the public, and many factors determine what information is accessible, including the charge, the sentence, current status, and length of time since sentence completion. By way of illustration, information would be publicly accessible if the record subject has been convicted of a crime punishable by a sentence of 5 years or more, or convicted of any crime and sentenced to a term of incarceration. In addition, at the time of the access request, the record subject must—

- be incarcerated, or
- be on probation, or
- be on parole, or
- having been convicted of a misdemeanor, has been released from incarceration, probation, parole, or supervision for not more than 1 year, or
- having been convicted of a felony, has been released from incarceration, probation, parole, or supervision within the last 2 years, or
- having been sentenced to the custody of the Department of Correction, has finally been discharged therefrom, either having been denied release on parole or having been returned to penal custody for violating parole for not more than 3 years.

CHSB certifies applicants for access to nonpublicly available criminal history information if the requestor (a) qualifies as a criminal justice agency; (b) is an agency or individual authorized to have access by State law; and/or (c) it has been determined that the public interest in disseminating such information clearly outweighs individual privacy interests. More than 6,000 noncriminal justice agencies in Massachusetts are authorized to access criminal records. For example, parents can seek access to all conviction and pending case information on prospective daycare providers with the written notarized consent of the record subject; however, parents are prohibited from disclosing any results of the criminal history check to third parties.

Access to sex offender information is governed by separate rules. Subject to several specific limitations, certain information is available about sex offenders classified by the Massachusetts Sex Offender Registry Board as posing a moderate or high risk (after the offender has an opportunity for administrative evidentiary proceedings). Included with all information provided is language cautioning that the misuse of sex offender information for purposes of harassment or discrimination is prohibited.

e. Federal and State statutes authorizing or requiring criminal background checks

A number of Federal statutes, including several enacted following the September 11 terrorist attacks, authorize or require the conduct of criminal background checks for purposes such as employment or volunteer services, firearms purchases, and housing. Following are some examples.

Federal employment statutes include—

- The Port and Maritime Security Act, signed into law on November 25, 2002, which requires background checks for persons with unrestricted access to controlled areas in maritime facilities, or to security-sensitive information, as designated by the Secretary of Homeland Security.[243]
- The Bioterrorism Preparedness Act of 2002, signed into law on June 12, 2002, which requires reviews to determine whether persons should be granted access to certain biological agents and toxins.[244]
- The Aviation and Transportation Security Act, signed into law on November 19, 2001, which creates numerous background check requirements, including for airport security personnel, airport and airline employees, individuals with access to secure areas of airports, Federal air marshals, and other transportation security personnel.[245]
- The USA PATRIOT Act, signed into law October 26, 2001, which requires or authorizes background checks for screeners and airport/airline employees, certain individuals seeking entry into the United States, and applicants for hazardous materials licenses.[246]

mation from the Massachusetts Criminal History Systems Board and the Massachusetts Sex Offender Registry Board.

[243]Pub. L. No. 107-295; 47 U.S.C. § 70105.

[244]Pub. L. No. 107-188.

[245]Pub. L. No. 107-71.

[246]Pub. L. No. 107-56.

- The National Child Protection Act of 1993,[247] as amended, which authorizes States and qualified entities, such as schools or youth-serving nonprofit organizations, to make nationwide background checks based upon fingerprint-based identification to determine if a care provider has been convicted of a crime that bears upon the provider's fitness to have responsibility for the safety and well-being of children, the elderly, or individuals with disabilities.[248] Federal law also requires background checks for employees in childcare centers located on certain Federal properties (such as executive branch agencies).[249]
- The Security Clearance Information Act of 1985 (SCIA),[250] which created a Federal standard authorizing the Central Intelligence Agency, the Office of Personnel Management, the Department of Defense, and the FBI to access criminal history information for background checks for security clearances and placement of people in national security duties.
- The requirement that employers operating nuclear facilities fingerprint employees and, through the U.S. Nuclear Regulatory Commission, submit the fingerprints to the FBI for criminal background checks.[251]
- Federal law also authorizes certain employers in the financial services sector to submit employee fingerprints for background checks,[252] and requires that members of national securities exchanges, brokers, dealers, and others, submit fingerprints to the FBI so that criminal history background checks can be performed.[253]

Federal statutes related to the purchase of firearms include—

- The Brady Handgun Violence Prevention Act,[254] which requires background checks to determine an individual's eligibility for certain firearms purchases. Brady checks consider disqualifying criminal history information as well as a range of other disqualifying factors, such as the individual's adjudication as a mental defective, use of a controlled substance, or dishonorable military discharge.

Federal public housing statutes include—

- Federal law that permits public housing authorities to request nationwide background checks on tenants.[255]

Similarly, State laws authorize or require criminal background checks for various licensing and employment purposes, such as for lawyers; mortgage brokers; and school employees who will have unsupervised access to children. Statutorily authorized checks can serve as the basis for conducting a nationwide criminal check using the III system. In addition, in States where access to information contained in the State repositories is not publicly available, authorization by State statute is necessary to access information held by the repository.

f. Sex offender registry information

Over the past 10 years, every State has developed a sex offender registry intended to provide increased public and law enforcement awareness of sex offenders in the communities where they live. The registries, which are often maintained by State criminal history repositories, contain information about designated sex offenses (which vary by State), but also can contain other information, such as a registrant's current address and an assessment of the level of risk that the registrant poses to the community. As of January 2004, all 50 States and the District of Columbia had centralized sex offender registries and 45 States and the District of Columbia had Internet sites devoted to their sex offender registries, most of them searchable.[256] In States that are legally permitted to put offender information on the Internet, and have done so, commercial vendors can use those systems as an additional resource for information products.

[247]Pub. L. No. 103-209 (Dec. 20, 1993).

[248]42 U.S.C. § 5119a(a); Volunteers for Children Act, Pub. L. No. 105-221 §§ 221-222 (Oct. 9, 1998) 112 Stat. 1885 (amending 42 U.S.C. § 5119a).

[249]Pub. L. No. 107-217 (Aug. 21, 2002).

[250]Pub. L. No. 99-169 (1985) codified in part at 5 U.S.C. § 9101.

[251]42 U.S.C. § 2169(a).

[252]5 U.S.C. § 9101.

[253]15 U.S.C. § 78(q)(f)(2).

[254]Pub. L. No. 103-159 (Nov. 30, 1993).

[255]*See* Pub. L. No. 104-120; 42 U.S.C. § 1437d(q).

[256]*See* SEARCH Law and Policy State Sex Offender Registry Web site, available at <http://www.search.org/programs/policy/registries.asp> (visited June 28, 2004).

2. Access to criminal history information maintained by courts

a. Presumption of open public access to court records

In addition to the information maintained in Federal and State repositories, pieces of an individual's criminal history record are also held in "open record" files maintained by police agencies and the courts. These original records of entry describe formal detentions and arrests, and can include incident reports, arrest reports, case reports, and other information that document that an individual has been detained, taken into custody, or otherwise been formally charged. Records of court proceedings include indictments, arraignments, preliminary hearings, pretrial release hearings, and other court events that, by law and tradition, are open to public inspection.[257]

As stated by the Conference of Chief Justices and Conference of State Court Administrators in October 2002:

> Historically, most court files have been open to anyone willing to come down to the courthouse and examine the files. The reason that court files are open is to allow the public to observe and monitor the judiciary and the cases it hears, to find out the status of parties to cases, for example dissolution of marriage, or to find out final judgments in cases.[258]

Moreover, the Federal and State laws and regulations that generally restrict the use of criminal history information contained in repositories maintained by executive branch agencies to criminal justice purposes "do not extend to information once it becomes part of a court record in a case, nor do they extend to court records containing criminal conviction information."[259] Accordingly, as noted above, the primary source of criminal history information for commercial vendors is the court system.

This presumption of open access to court files is rooted in the common law and in constitutional principles. The U.S. Supreme Court has recognized a fundamental common law right "to inspect and copy public records and documents, including judicial records and documents."[260] This right is not absolute, however: "[E]very court has supervisory power over its own records and files, and access has been denied where court files might have become a vehicle for improper purposes."[261] Courts have cited various reasons underlying the tradition of open court records, including, for example, to aid in preserving the integrity of the judicial process; to enhance the public trust and confidence in the judicial process; to insulate the process against attempts to use the courts as tools for persecution; and to maintain public trust and confidence in the operation of the court system.[262]

Open access to court records is also rooted in constitutional principles. One of the seminal public access decisions by the U.S. Supreme Court, decided on constitutional grounds, is *Richmond Newspapers Inc.* v. *Virginia*.[263] The case arose from a dispute not over public access to records, but rather over the ability of the public (actually, the press) to attend a criminal trial that had been closed at the request of the defendant, with the consent of the prosecutor and the agreement of the trial court. The trial was closed pursuant to a State statute that permitted closure of a trial under certain circumstances. The Supreme Court of Virginia upheld the trial closure, but the U.S. Supreme Court reversed that decision on appeal.

In the *Richmond Newspapers* case, the Court analyzed the evolution of the criminal trial in the Anglo-American legal system, concluded that what "is significant for present purposes is that throughout its evolution, the trial has been open to all who cared to observe,"[264] and found that there is a first amendment right of access to criminal trials.[265] Concurring opinions in the case further

---

[257]Privacy Task Force report, *supra* note 106, at pp. 13–14.

[258]Martha Wade Steketee and Alan Carlson, *Developing CCJ/COSCA Guidelines for Public Access to Court Records: A National Project to Assist State Courts* (National Center for State Courts and The Justice Management Institute, Oct. 18, 2002) at 1. Hereafter, CCJ/COSCA Guidelines.

[259]Ibid., at p. 47.

[260]*Nixon* v. *Warner Communications, Inc.* 435 U.S. 589 (1978).

[261]Ibid., at 596.

[262]Susan Larson, "Public Access to Electronic Court Records and Competing Privacy Interests," *Judgelink* (Jan. 9, 2003) at p. 1, citing *United States* v. *Hickey*, 767 F.2d 705, 708 (10th Cir. 1984) (hereafter, Larson article); *Williams* v. *Stafford*, 589 P.2d 322, 325 (Wyo. 1979); Vermont Rules for Public Access to Court Records, § 1 Reporter's Notes.

[263]448 U.S. 555 (1980).

[264]Ibid., at 564.

[265]Ibid., at 576–77.

illuminate the scope of the Court's decision. Thus, for example, Justice Stevens stated that the "First Amendment protects the public and the press from abridgement of their rights of access to information about the operation of their government, including the judicial branch."[266] But, Justice Brennan emphasized that the right of access is not absolute: "[O]ur decisions must…be understood as holding only that any privilege of access to governmental information is subject to a degree of restraint dictated by the nature of the information and countervailing interests in security or confidentiality."[267]

b. General description of court procedures concerning record access

The general rule remains that court records, including those in criminal cases, are open to the public; however, individual jurisdictions and individual courts are responsible for determining the particulars of how to implement that rule. Thus, historically, the procedures governing access to court records have varied from jurisdiction to jurisdiction. In most States, courts exercise control over their records and define public access rules under their general supervisory powers, which include the authority to prevent improper use of such records.[268] In some States, however, legislatures play a role in setting court record-access law.[269]

Generally, all documents filed with a Federal court are public records and are available through the clerk's office, although some documents are sealed by special court order, and some documents are confidential by operation of law, such as grand jury materials and criminal files relating to juveniles.[270] In recent years, the Judicial Conference of the United States, which is the principal policymaking body for the Federal court system, has been addressing issues related to public and private access to electronic records in all Federal courts.[271]

While historically court files have been open, technological innovations have made the question of public access substantially more complex than in the past, when individuals had to go to the courthouse and wade through volumes of paper or sit through a trial to obtain access to court-held information. Not only are court records now available in electronic form—which allows for easier and broader public access—but data from electronic records can be compiled in new ways, and bulk access allows entire databases to be copied. Moreover, Internet access to court records allows greater numbers of people to more easily review potentially sensitive information contained in court records, thus threatening to eliminate the "practical obscurity" of paper court records that previously could have been said to provide some measure of privacy protection for court participants.[272]

In attempting to balance the competing interests posed by new technologies, privacy interests, and historical principles of openness, the courts have grappled with several questions. For example, should different access rules apply to paper as opposed to electronic records? Should different rules apply to different types of records (for example, to court opinions versus records of court proceedings)? Should distinctions be drawn between criminal and civil cases? How can sensitive information be defined and protected in otherwise accessible records? Is it appropriate to charge for online access to records? Should cost or access distinctions be made depending upon who requests the records (for example, lawyers versus ordinary citizens, or citizens versus commercial vendors)? Should data be available in bulk?

At present, there is a wide variety of responses to these questions. While many committees and organizations have begun to study public access issues and publish recommendations and guide-

[266]Ibid., at 584 (Stevens, J., concurring).

[267]Ibid., at 586 (Brennan, J., concurring). *But see Paul* v. *Davis*, 424 U.S. 693, 713 (1976), which held that the Constitution does not recognize a privacy interest in the dissemination by criminal justice agencies of information about official acts, such as arrests.

[268]Larson article, *supra* note 262, at p. 2, citing *Nixon* v. *Warner Communications*, 435 U.S. 589 (1978).

[269]*See*, *for example,* Va. Code Ann. § 16.1-69.54, et seq.

[270]*See* Web site of the U.S. Courts, available at <www.uscourts.gov/faq.html>.

[271]*See*, *for example, Report of the Judicial Conference Committee on Court Administration and Case Management on Privacy and Public Access to Electronic Case Files*, Judicial Conference of the United States, Jan. 8, 2003, available at <www.privacy.uscourts.gov/Policy.htm> (visited June 28, 2004). Hereafter, Judicial Conference Committee report.

[272]Larson article, *supra* note 262, at p. 1.

lines,[273] the adoption of policies and promulgation of rules by courts is still in a state of flux.[274]

Discussed below are the guidelines for public access to court records adopted by the Conference of Chief Justices and Conference of State Court Administrators to assist State courts, followed by brief descriptions of how two States have recently addressed the issues raised by public access to court records in light of technological advances.

— Chief justices/State court administrators guidelines for public access to court records

In order to provide guidance to State judiciaries and local courts on how to address the myriad policy issues related to public access to court records in the current environment, the Conference of Chief Justices/Conference of State Court Administrators (COCJ/COSCA) published guidelines on the subject in October 2002. As explained in the introduction, new access policies may be required for several reasons:

> Technological innovations have resulted in more court records being available in electronic form and permit easier and wider access to the records that have always been available in the courthouse. Information in court records can now be "broadcast" by being made available through the Internet. Information in electronic records can be easily compiled in new ways. An entire database can be copied and distributed to others. At the same time not all courts have the same resources or that same level of technology, resulting in varying levels of access to records across courts in the same state.[275]

The guidelines are intended to address the concern that "the proper balance is maintained between public access, personal privacy, and public safety, while maintaining the integrity of the judicial process."[276] Moreover, the guidelines seek to provide a comprehensive framework for a policy on public access to court records, providing for access in a manner consistent with 11 "significant" public policy interests:

1. maximize accessibility to court records
2. support the role of the judiciary
3. promote governmental accountability
4. contribute to public safety
5. minimize risk of injury to individuals
6. protect individual privacy rights and interests
7. protect proprietary business information
8. minimize reluctance to use the courts to resolve disputes
9. make most effective use of court and clerk of court staff
10. provide excellent customer service
11. avoid unduly burdening the ongoing business of the judiciary.[277]

The CCJ/COSCA guidelines are based on five underlying premises:

- The traditional policy that court records are presumptively open to public access should be retained.
- Generally, access should not depend upon whether a court record is in paper or electronic form.
- The nature of certain information in some court records is such that while public access at the courthouse is maintained, remote public access

[273] *See*, *for example,* CCJ/COSCA Guidelines, *supra* note 258, Privacy Task Force report, *supra* 106.

[274] *See* Center for Democracy & Technology, "A Quiet Revolution in the Courts: Electronic Access to State Court Records: A CDT Survey of State Activity and Comments on Privacy, Cost, Equity and Accountability" (Aug. 21, 2002), which includes a State-by-State summary of the type of electronic access provided as of July 1, 2002. Available at <www.cdt.org/publications /020821courtrecords.shmtl> (visited June 28, 2004). *See also*, Reporters Committee for Freedom of the Press, "Electronic Access to Court Records: Ensuring Access in the Public Interest," which also includes a State-by-State discussion, current as of November 2003, available at <www.rcfp.org/courtaccess /viewstates.cgi> (visited June 28, 2004). *See also*, ABA Journal E-Report, "Florida Court Orders Records Offline" (Jan. 9, 2004) available at <www.abanet.org/journal/ereport> (visited Jan. 20, 2004), reporting on (1) a November 2003 Florida Supreme Court order limiting the accessibility of certain court records in the Florida State courts and establishing a committee on privacy and court records to work on a statewide policy to protect privacy rights, and (2) a Butler County (Ohio) court order requiring that domestic relations cases be removed from court Internet sites.

[275] CCJ/COSCA Guidelines, *supra* note 258, at p. 1.

[276] Ibid.

[277] Ibid., at p. 4.

to the information in electronic form may be inappropriate.

- The nature of the information in some records is such that all public access should be precluded unless authorized by a judge.
- Access policies should be clear, consistent, and not subject to interpretation by individual court or clerk personnel.[278]

Consistent with the stated public policies and underlying premises, the general rule, as stated in the guidelines, is that information in court records is accessible to the public, except as specifically prohibited.[279] The prohibitions are for information that is not accessible pursuant to Federal law, State law, court rule, or case law (which should be identified in the rule)[280] and information to which the court has prohibited access.[281] Information included in this inaccessible category could include, for example, information from types of cases for which records are generally not made public (for example, juvenile cases, adoption proceedings, mental health cases, guardianship, or conservatorship proceedings), and documents or information for which privacy or security concerns may dictate confidentiality (for example, contact information of witnesses in sexual assault cases, account numbers, medical or mental health records, search warrants, investigatory files, and public employee personnel records). As the guidelines note, the categories of restricted information vary considerably across the States.[282]

The guidelines are intended to apply to all court records, defined broadly to include what is traditionally considered the "case file," other information created by the court that may or may not be in the case file (for example, index, docket, calendar, record of proceedings), and information that relates to the operation of the court, but not to a specific case.[283]

The guidelines provide, generally, that access to public records should be the same for the general public, the media, and the information industry.[284] How access is permitted, however, may vary depending upon the type of information, and there may be exceptions to equal access depending upon the intended uses of the information.

For example, the guidelines provide that the types of general information in court records that have traditionally been given wider public distribution—such as litigant/party indexes, listings of new case filings (including party names), register of actions showing what documents have been filed in a case, calendars or dockets, judgments, orders and decrees, and liens affecting title to real property—should be made remotely accessible to the public if they exist in electronic form.[285]

The guidelines also provide that by contrast, other records, to be specifically identified by the jurisdiction, could be made publicly accessible only at a court facility, rather than remotely.[286] This provision—which could be used to protect information such as contact information, Social Security numbers or account numbers, and medical records (if access is not altogether prohibited)—is intended to reduce the risk of negative impacts from public accessibility, while maintaining traditional public accessibility at the courthouse. The guidelines also identify alternative means of achieving this objective, such as allowing remote access only through a subscription service, or

[278]Ibid., at p. 1.

[279]Ibid., at Section 4.10.

[280]Ibid., at Section 4.60.

[281]Ibid., at Section 4.70. This guideline provides that requests can be made to prohibit access to information in a court record, or to permit access to information that has been restricted, and the standards to be used by the court in ruling on such requests. Ibid.

[282]Ibid., at Section 4.60 Commentary.

[283]Ibid., at Section 3.00 and Commentary.

[284]Ibid., at Section 2.00 Commentary. "Public" excludes, however, court employees or agents, public agencies whose access to court records is defined by statute, rule, order or policy, and parties to a case and their lawyers, regarding access to the court record in their case. Ibid., at Section 2.00(e).

[285]Ibid., at Section 4.20. The guidelines define "remote access" as "the ability to electronically search, inspect, or copy information in a court record without the need to physically visit the court facility where the court record is maintained." Ibid., at Section 3.30. The term is intended to be "technologically neutral," that is, independent of any particular technology or means of access, for example, the Internet or a dial-up system such as the Federal court's PACER system. PACER (Public Access to Court Electronic Records) is the automated case management information system used by the Federal courts to provide information about court cases that can be accessed remotely by a subscriber. *See* discussion in the "Access to court records in the Federal courts" section later in Part II.

[286]Ibid., at Section 4.50.

limiting remote access to one case at a time.[287]

The guidelines provide for public access to "compiled information" from court records, defined as "information that is derived from the selection, aggregation or reformulation by the court of some of the information from more than one individual court record."[288] Any member of the public may request compiled information that consists solely of information that is publicly accessible, as well as information that is restricted, if requested for scholarly, journalistic, political, governmental, research, evaluation, or statistical purposes.[289] The Commentary acknowledges that generating compiled data may require court resources and compete with normal operations of the court, and notes that it may be less burdensome and less costly for a court to provide bulk distribution of the requested information.[290]

The guidelines address the issue of handling requests for large volumes of information in court records, as opposed to requests on a case-by-case basis, under its bulk distribution rule.[291] That rule provides that bulk distribution, defined as "the distribution of all, or a significant subset, of the information in court records, as is and without modification or compilation," is permitted for court records that are publicly accessible, and can be requested for any purpose (records that are not publicly available may be made available for scholarly, journalistic, political, governmental, research, evaluation, or statistical purposes).[292] The Commentary notes that there are dangers inherent in permitting bulk transfers of data into databases beyond the court's control because over time, the information will likely become incomplete, inaccurate, stale, or contain information that has been removed from the court's records, thus requiring the court to periodically "refresh" or update the information. In addition, with respect to criminal conviction information, bulk distribution could make it impossible to implement expungement policies.[293]

The Commentary rejected limitations on bulk access, in part on technology grounds: "[m]any states that have considered the bulk data issue for information in electronic form have adopted access policies that only allow case-by-case access, one case at a time, and no bulk distribution, even of otherwise publicly accessible information. However, existing technology and software, using repeated queries and 'screen scraping,' can accomplish bulk distribution from 'one-case-at-a-time' systems fairly rapidly. The CCJ/COSCA Guidelines, therefore, explicitly provide for bulk distribution in recognition of this potential."[294]

While the guidelines do not address methods for ensuring the continuing accuracy of data distributed in bulk, they note that many States have adopted policies that allow access to one case at a time but prohibit bulk access to reduce the stale information problem and to eliminate the need to adopt mechanisms for periodically updating data. Some have also allowed bulk access for only particular types of information, such as indexes.[295] Alternatively, the guidelines note that the requestor of bulk information could be held responsible for the currency and accuracy of the information before making it accessible to its clients or the public, or the requestor could be required to inform clients or the public of the limitations of the data.[296]

Finally, the guidelines recognize that providing access to information in court records is not without cost, which must be absorbed by either the taxpayers in funding the courts or those requesting ac-

[287]Ibid., at Section 4.50 Commentary.

[288]Ibid., at Section 4.40(a).

[289]Ibid., at Section 4.40(c).

[290]Ibid., at Section 4.40 Commentary.

[291]Ibid., at Section 4.30.

[292]Ibid.

[293]Ibid., at Commentary. The Commentary also notes a "counter-intuitive aspect" of bulk data release: "In order to correctly link court information with information from other sources, the information vendor must have pieces of information that allow accurate matching of court information about someone or an entity with information from other sources. This type of personal identifier information is often the most sensitive in terms of privacy. If a court were interested in minimizing the risk of bulk data it provides being incorrectly linked to information from other sources, it might provide more personal identifier information, not less, in those situations where linking is contemplated." Generally, court records do not contain key linking information, such as birth dates or Social Security numbers.

[294]Ibid.

[295]Ibid.

[296]Ibid. The guidelines also recognize another concern with bulk distributions; that is, the extent to which electronic records may be "an atypical subset" of data from all court records, because, for example, the distribution may include information only after a certain date (when electronic records became available), or only complex or certain types of cases.

cess.[297] The guidelines thus provide that a court may charge a fee for access to court records in electronic form, for remote access, or for bulk distribution or compiled information. The Commentary cautions, however, that any fee "should not be so prohibitive as to effectively deter or restrict access or create unequal access to court records."

— Example: New rules governing access to electronic records in California trial courts

Following a 6-year program of guidance, the Judicial Council of California approved new rules, effective July 1, 2002, applicable to all California superior courts (that is, trial courts), and governing public access to electronic court records. As summarized by the Judicial Council, the rules "permit broad electronic access to most civil records while restricting remote Internet access in criminal records and other cases that are likely to contain sensitive personal information."[298] The rules are intended to "provide the public with reasonable access to trial court records that are maintained in electronic form, while protecting privacy interests."[299] Thus, as the Council's Court Technology Advisory Committee commented:

> The rules acknowledge the benefits that electronic court records provide but attempt to limit the potential for unjustified intrusions into the privacy of individuals involved in litigation that can occur as a result of remote access to electronic court records. The proposed rules take into account the limited resources currently available in the trial courts. It is contemplated that the rules may be modified to provide greater electronic access as the courts' technical capabilities improve and with the knowledge gained from the experience of the courts in providing electronic access under these rules.[300]

The new California rules are generally consistent with the CCJ/COSCA guidelines. They begin with a statement of the "general right of access"—specifically, that "all electronic records must be made reasonably available to the public in some form, whether in electronic or in paper form, except those sealed by court order or…made confidential by law."[301] They provide that if a court maintains electronic records of certain basic information, the court must provide electronic access to them, through both computer terminals at the courthouse and remotely over the Internet, "to the extent it is feasible to do so." The basic information includes "registers of actions," calendars and indexes, and other records in civil cases, with certain enumerated exceptions.[302] In addition, if a court maintains electronic records other than calendars, registers, and indexes, it must provide electronic access to them both remotely and at the courthouse to the extent feasible, but it must do so only on a case-by-case basis.[303]

Records in criminal and juvenile cases, as well as records in those civil cases involving family law, guardianships or conservatorships, mental health, or civil harassment, must be available electronically at the courthouse, but they will not be available remotely; in such cases, only the register of actions, calendars, and indices will be available remotely.[304] The Advisory Committee commented that while it recognized the records in such cases are public records that should be available at the courthouse, either in paper or electronic form, it noted that, "they often contain sensitive personal information [and] the court should not publish that information over the Internet."[305] The case-by-case limitation does not apply to access

[297]Ibid., at Section 6.00 Commentary.

[298]"New Rules Expand Public Access to Electronic Trial Court Records," News Release No. 91 (Judicial Council of California, Dec. 18, 2001) at p. 1.

[299]California Rules of Court, Rule 2070(a)

[300]Ibid., Advisory Committee Comment.

[301]Ibid., at Rule 2073(a).

[302]Ibid., at Rule 2073(b). The register of actions is a form of docket sheet, listing the case title, the date it began, and each subsequent proceeding in the action. Providing electronic access "to the extent feasible" is defined to mean the extent that a court determines it has the resources and technical capability to provide electronic access. Rule 2073(d). *See also* Rule 2077, which identifies information that must be included in calendars, indexes, and registers of actions, as well as information (such as, Social Security numbers and victim and witness information) that must be excluded.

[303]Ibid., at Rules 2073(b)(2) and 2073(e).

[304]Ibid., at Rule 2073(c).

[305]Ibid., at Advisory Committee Comment.

to calendars, registers of actions, or indexes.[306]

The provision that access may be granted to an electronic record (other than the register, calendars, or indexes) only when the record is identified by the case number, caption, or party name, *and* only on a case-by-case basis, addresses, in part, the issue of bulk distribution. Bulk distribution is permitted only of a court's electronic calendar, register of actions, and index.[307] The Advisory Committee's rationale for these limitations on bulk distributions is as follows:

> These limitations are based on the qualitative difference between obtaining information from a specific case file and obtaining bulk information that may be manipulated to compile personal information culled from any document, paper, or exhibit filed in a lawsuit. This type of aggregate information may be exploited for commercial or other purposes unrelated to the operations of the courts, at the expense of privacy rights of individuals.[308]

The rules permit courts to condition electronic access on (1) the user's consent to access the records only as instructed by the court, and (2) the user's consent to the court's monitoring of access.[309] The courts must provide appropriate notice of such conditions, and may deny access to any person for failure to comply with them.[310] Finally, the courts may impose fees for the costs of providing public access to its electronic records, according to a fee schedule provided by law.[311]

— Example: Access to court records in Washington State

By statute in the State of Washington, the Judicial Information System (JIS) provides case management automation to the courts, and has responsibility for maintaining the automated statewide judicial information system.[312] By statute, through the Judicial Information System Committee (JISC), the courts are required to—

- implement processes for making judicial information available electronically
- promote and facilitate electronic access to the public of judicial information
- consider electronic public access needs when planning new, or upgrades to existing, information systems
- develop processes to determine which judicial information the public most wants and needs
- increase capabilities to receive information electronically from the public and transmit forms, applications, and other communications and transactions electronically
- use technologies that allow continuous access 24 hours a day, 7 days per week, involve little or no cost to access, and are capable of being used by persons without extensive technology ability.[313]

Like many other States, Washington's access policies for court records are in a state of flux. The JISC data dissemination policy currently in effect, which governs access only to electronic records, allows the public case-by-case access to "any electronic record that is a reflection of the legal file," including index data (i.e., filing date, case caption, party name and relationship to the case, cause of action or charge, law enforcement agency, case number, case outcome, and case disposition date).[314] In general, case-specific records in electronic form are available "to the extent that such records in other forms are open to inspection by statute, case law and court rule," unless restricted by certain enumerated

[306]Ibid., at Rule 2073(e). But, as noted, Rule 2077 does provide for the exclusion of certain information from registers, calendars, and indexes.

[307]Ibid., at Rule 2073(f). "Bulk distribution" is defined as distribution of all, or a significant subset, of the court's electronic records. Ibid.

[308]Ibid., at Advisory Committee Comment.

[309]Ibid., at Rule 2074(c).

[310]Ibid.

[311]Ibid., at Rule 2076.

[312]Revised Code of Washington, RCW Chapter 2.68.

[313]Revised Code of Washington, RCW § 2.68.050.

[314]"Summary of [JISC Data Dissemination] Policy," available at <www.courts.wa.gov/dataDis/?fa=datadis.policySummary> (visited June 28, 2004). *See also,* JISC Data Dissemination Policy at Section III, available at <www.courts.wa.gov/dataDis/?fa=datadis.policyDiss>. This JISC policy was promulgated pursuant to JISC Rules, which declare "the policy of the courts [is] to facilitate public access to court records, provided such disclosures in no way present an unreasonable invasion of personal privacy and will not be unduly burdensome to the ongoing business of the courts." JISC Rule 15.

privacy and confidentiality policies.[315]

Certain personal identifying information cannot be released, such as witness, juror, and party contact information, and personal identity numbers, such as Social Security numbers and bankcard numbers.[316] Information is also not available on sealed cases, or those deemed confidential, such as cases relating to adoption, mental illness, juveniles, and the like.[317] Data for a research report may be provided "when the identification of specific individuals is ancillary to the purpose of the research, the data will not be sold or otherwise distributed to third parties, and the requester agrees to maintain the confidentiality required (e.g., use security provisions such as passwords and encryption, keep confidential any identifying data, and agree not to copy or duplicate data other than for stated research purposes)…."[318] In addition, the policies provide the following, with respect to the availability of "contact lists":

> Access to JIS information will not be granted when to do so would have the effect of providing access to lists of individuals for commercial purposes, … i.e., that in connection with access to a list of individuals, the person requesting the record intends that the list will be used to communicate with the individuals named in the record for the purpose of facilitating profit expecting activity.[319]

The current policy also prohibits "direct downloading" of the JIS database, except for index items, and such downloads are subject to a data dissemination contract.[320] Similarly, access of an individual to "compiled reports on an individual," defined as "based on information related to more than one case or more than one court," must be limited to the items contained in a case index.[321]

As a practical matter, notwithstanding these JISC policies, actual public access to court records in Washington is quite variable, depending upon where and how one seeks such access.[322] The only data available remotely, through the JIS under the policies described above, is basic case information in indexes, docket sheets, and the like; images of actual case documents are not available through that system. Moreover, access to JIS data is by subscription, pursuant to prescribed fees. These same "index-type" data are also available electronically at the courthouse, where public computer terminals are available for access. Again, case documents are not available through the JIS.

Some courts have their own relatively extensive databases, including actual case documents, which may be available electronically at the courthouse or remotely via the court's Web site. What may be available, and how, varies greatly from court to court.

In July 2003, the JISC proposed for comment a new rule addressing public access to electronic information. According to the statement accompanying the proposed rule released for comment:

> The rule informs and instructs the courts, practitioners, and the public about access to court records. The eventual placement of court records on public websites necessitates the adoption of this rule. The rule was developed with the understanding that courts are public institutions and that most court records should be available for public inspection whether the records are obtained at the court house or though the internet. However, the rule does recognize that certain court proceedings are not publicly accessible and records from these proceedings should not be available to the general public.[323]

The proposed rule is generally consistent with the CCJ/COSCA guidelines, providing, among other things, for regulation of bulk and compiled distribution of data.[324] Although comments have

[315]JISC Data Dissemination Policy, Section III.B.3.

[316]Ibid., at Section IV.B.

[317]Ibid., at Section IV.A.

[318]Ibid., at Section IV.C.

[319]Ibid., at Section III.A.5.

[320]Ibid., at Section III.A.2.

[321]Ibid., at Section III.A.3. Individuals may request such a report on themselves, however, if they sign a privacy waiver. Ibid., at Section III.B.4.

[322]We rely herein on discussions held on Apr. 15, 2003, with the Data Dissemination Administrator in the Washington Administrative Office of the Courts.

[323]*See* Court Rules Committee's Suggested New Rule GR 31, "Access to Court Records," available at <www.courts.wa.gov/court_rules/proposed/2003July/GR_31.doc> (accessed June 28, 2004).

[324]Ibid.

been submitted, no action has yet been taken on the draft rules. Moreover, the policies stated in the proposed rule may be somewhat ahead of the data that may actually be available, at this time, in many Washington jurisdictions.

— Access to court records in the Federal courts

As the principal policymaking body for the Federal court system, the United States Judicial Conference has been examining issues related to privacy and public access to electronic case files since 1999. In September 2001, beginning with the general principle that "Federal court case files, unless sealed or otherwise subject to restricted access by statute, federal rule, or Judicial Conference policy, are presumed to be available for public inspection and copying," the Conference adopted a policy that it believed could provide solutions to the privacy and access issues presented by the use of electronic records and electronic communications in the Federal courts.[325]

With respect to civil case files, the Conference provided for liberal remote electronic access to civil case files while providing for some privacy protection. The Conference recommended that documents in civil case files should be made available electronically to the same extent that they are available at the courthouse, with two exceptions: Social Security case files should not be available, and litigants should be required to modify or partially redact certain "personal data identifiers" (such as, Social Security numbers, dates of birth, financial account numbers, and names of minor children) from case documents, whether electronic or hard copy.[326] Clearly, this policy will require counsel and *pro se* litigants to protect their interests, and will depend on the judicial discretion to protect privacy and security issues as they arise in cases. But the Conference noted that the experience of Electronic Case Filing prototype courts has not been problematic, and that as to those courts that had been making their case file information available through the Internet using PACER, "there have been virtually no reported privacy problems as a result."[327] The Conference explained that the civil case file policy is simple and can be easily and consistently applied nationwide. It stated that the policy:

> [W]ill 'level the playing field' in civil cases in federal court by allowing attorneys not located in geographic proximity to the courthouse easy access. Having both remote electronic access and courthouse access to the same information will also utilize more fully the technology available to the courts and will allow clerks' offices to better and more easily serve the needs of the bar and the public.[328]

The Judicial Conference also offered this comment about the impact of its policy on commercial vendors:

> [This policy] might also discourage the possible development of a 'cottage industry' headed by data resellers who, if remote electronic access were restricted, could go to the courthouse, copy the files, download the information to a private website, and charge for access to that website, thus profiting from the sale of public information and undermining restrictions intended to protect privacy.[329]

As to criminal cases, the Judicial Conference initially recommended that remote public electronic access to documents in criminal cases should not be available, with the express understanding that the policy would be re-examined within 2 years.[330] It based this recommendation on the determination that any benefits from remote access to criminal files would be outweighed by the safety and law enforcement risks that could be created. The Conference cited two examples of such risks—

1. Defendants and others could learn about cooperation and other activities of defendants (such as the details of a de-

[325]Judicial Conference Committee report, *supra* note 271, at p. 1.

[326]Ibid., at p. 5. The Judicial Conference adopted a similar policy with respect to bankruptcy case files.

[327]Ibid., at p. 3. As noted, PACER is the fee-based electronic public access service that allows registered users to obtain case and docket information about a particular individual or case, from Federal Appellate, District, and Bankruptcy courts, and from the U.S. Party/Case Index. Many courts provide copies of documents in case files and users may conduct nationwide searches to determine whether or not a party is involved in Federal litigation. Currently, through PACER, most Federal courts are available on the Internet. *See* <http://pacer.psc.uscourts.gov /pacerdesc.html> (visited Apr. 5, 2004).

[328]Judicial Conference Committee report, *supra* note 271, at p.3.

[329]Ibid.

[330]Ibid., at p. 4.

fendant's involvement in the government's case) and that such information could be used to intimidate, harass, and possibly harm victims, defendants, and their families.

2. Routine remote access to criminal files could inadvertently increase the risk of unauthorized public access to preindictment information, such as unexecuted arrest and search warrants, which could severely hamper and compromise investigative and law enforcement efforts and pose a significant safety risk to law enforcement officials.[331]

Notwithstanding this recommendation, the Conference emphasized that opinions and orders (as determined by the court) and criminal docket sheets would still be available through court Web sites, PACER, and PACERNet, and that the recommendation would be reconsidered "if it becomes evident that the benefits of public remote access significantly outweigh the dangers to victims, defendants and their families, and law enforcement personnel."[332]

In March 2002, the Judicial Conference adopted two modifications to the prohibition on remote public access to electronic criminal case files.[333] The first modification was to allow such access in certain "high profile" cases; that is, "where demand for copies of documents places an unnecessary burden on the clerk's office." In such cases, remote access would be allowed only if the parties have consented to such access, and the presiding judge finds that such access is warranted by the circumstances.[334] The second modification was to create a pilot program to allow selected courts that had provided remote public access to criminal case files prior to the conference adoption of the prohibition to return to that level of access for the purpose of studying those courts and their experience.[335]

On January 15, 2004, the Administrative Office of the U.S. Courts announced that seven Federal courts were participating in a pilot program to make transcripts of courtroom proceedings available online. As part of this "experiment," the U.S. District Court for the District of Columbia will make transcripts of courtroom proceedings in criminal cases, as well as civil proceedings, available electronically.[336]

3. Access to corrections department records

In addition to information maintained in Federal and State repositories and the courts, criminal justice record information also is held by Federal, State, and local corrections departments and facilities. While these records focus on facts concerning current or past incarceration in particular facilities, they can also include information about an offender's offenses, court appearances, post-incarceration supervision (probation, parole, community service, etc.) or release, as well as personal information.

The availability of records maintained by the Federal Bureau of Prisons (BOP) is governed by the Privacy Act, the Freedom of Information Act (FOIA), and related Justice Department regulations. The primary information made available to the public is through the BOP's "Inmate Locator," which is available online. By entering a first and last name, or a prisoner identification number,[337] anyone can obtain limited information about individuals who have been Federal inmates at any

[331]Ibid. The Conference noted that sealing such information would not solve the problem because the mere fact that a document is sealed would signal probable defendant cooperation or covert law enforcement activities. Ibid., at pp. 4–5.

[332]Ibid., at p. 5.

[333]"Limited Exception to Judicial Conference Privacy Policy for Criminal Case Files," available at <www.privacy.uscourts.gov/amend.htm> (visited Apr. 5, 2004).

[334]This modification arose out of a temporary exception to the prohibition on remote access to criminal case files that had been prompted by the high number of media and public requests for copies of documents in the terrorist case of *U.S.* v. *Moussaoui*, now pending in the U.S. District Court for Eastern District of Virginia. *See* Administrative Office of the U.S. Courts, "Judicial Conference Approves Pilot Program for Remote Public Access to Criminal Case Files," News Release (Mar. 13, 2002) available at <www.uscourts.gov/Press_Releases/pr031302jc.pdf> (visited Apr. 5, 2004).

[335]Ibid. The pilot program included 11 courts, including the U.S. District Court for the District of Columbia. Administrative Office of the U.S. Courts, "Eleven 'Pilot' Courts Selected for Remote Public Access to Criminal Cases Files," News Release (May 7, 2002), available at <www.uscourts.gov/Press_Releases/pilotcts.pdf> (visited June 28, 2004).

[336]*See* Administrative Office of the U.S. Courts, "Pilot Project Makes Court Transcripts Available Onlline," available at <www.uscourts.gov/newsroom/pilot.htm> (visited Jan. 15, 2004).

[337]This can be the inmate's Federal Register number, the District of Columbia Department of Corrections (DCDC) number, FBI number, or INS number.

time since 1982.[338] The online system provides the inmate's full name; Federal BOP register number; current age (not date of birth, which is nonpublic information) or the fact that the inmate is deceased; race; sex; projected release date, if known (this can include release to another jurisdiction or to another sentence, not necessarily release into the community); the date released (which can include release on parole or other correctional supervision); and the inmate's location within the BOP system.[339] Additional information, including offenses and sentencing dates, is available to the public only through FOIA requests.[340]

State and local corrections departments also make inmate information available to the public, many by online "locators" similar to that run by the Federal system.[341] Although there is no uniformity, in many instances more information is available through these systems than through the Federal system. The availability of the information is governed by each State's public records laws and related regulations. The cost and availability of corrections data in bulk varies from State to State. By way of example, a few State online inmate locator programs are discussed below.

a. Florida

In keeping with its open records policy, the Florida Department of Corrections provides several searchable online databases containing substantial amounts of information about inmates in the Florida Prison System.[342] These databases include:

1. the inmate population (excluding those released, escaped, on probation or parole, or in county jails)
2. the supervised population (those on parole, probation, work release, or other types of "supervision")
3. inmates who have been released after October 1997, or are scheduled for release
4. inmates who have escaped from custody and have an outstanding arrest warrant
5. absconder/fugitives, consisting of offenders who have ceased to make themselves available for supervision.

Users can also perform a comprehensive search of all five databases.

Although several different identifiers can be entered in performing searches, users can obtain detailed information merely by entering the first two letters of a first and last name. The information provided through the search includes, for each individual matching the search request, a photograph, appearance information (race, gender, age, date of birth, weight, height, eye and hair color, and scars, marks, and tattoos), aliases, criminal history (including offenses, case numbers, sentencing information, past offenses, past incarceration, and supervision history), location within the system, release date(s), and for released inmates, their stated address upon release.[343] Depending upon the type of information, it is updated either weekly or daily. Some Florida county jails also provide inmate information online, including arrest information.[344]

b. Kentucky

The Kentucky Department of Corrections provides substantial online information about inmates in Kentucky institutions through the Kentucky Offender Online Lookup (KOOL) system.[345] Information about specific inmates can be obtained by entering a last name. In addition to photographs and personal appearance information, the system provides aliases,

---

[338] Inmates released before 1982 can be located via a written request, which must include the inmate's name (including middle initial), date of birth or approximate age at the time of incarceration, race, and approximate dates in prison.

[339] No State corrections information is available through the Federal BOP, even if a State inmate is housed in the Federal system.

[340] *See* <www.bop.gov>.

[341] At least 30 States have online inmate locator services. Another 18 States provide some amount of "offender information" via telephone or e-mail. *See, for example,* a listing of State corrections departments on Montana Department of Corrections Web site at <www.cor.state.mt.us/resources/states.asp> (visited Apr. 5, 2004). Only the States of Alaska and New Hampshire do not publicly offer a mechanism by which the public can obtain such information.

[342] *See* <www.dc.state.fl.us/inmateinfo/inmateinfomenu.asp> (visited Apr. 5, 2004).

[343] *See generally*, ibid.

[344] *See*, *for example,* Web site of Broward County Sheriff's Office, at <www.sheriff.org>, which provides personal and arrest information, on individuals incarcerated in the Broward County jail, updated every 15 minutes (visited Apr. 5, 2004).

[345] *See* the Kentucky Department of Corrections' Web site, at <www.corrections.ky.gov/kool/ioffsrch.asp> (visited June 28, 2004). The relevant statutes governing release of such information are K.R.S. Ch. 17.150 and 61.870 et seq.

when the offender entered the system, location in the system (including community service, and assignment to facilities other than prisons), criminal history (indictment numbers, crime dates, offenses (up to 10), conviction dates, and location), and parole hearing information. The Kentucky system includes only currently incarcerated offenders; it does not provide release dates, information about former inmates, or information about persons currently on probation or parole.[346]

c. New York

The New York State Department of Correctional Services provides an online "inmate lookup" service, but it contains less information than either Kentucky or Florida.[347] Information is provided on "everyone sentenced to State prison since the early 1970s," except youthful offenders and persons whose convictions have been set aside by a court.[348] According to the Department of Correctional Services' Web site, information is provided on former inmates "primarily so an inquiry regarding a released inmate results in a positive result telling when and why the inmate was released."[349]

The New York inmate database can be accessed by entering a partial or full last name. The personal information provided is limited to name, sex, date of birth, and race/ethnicity. The custody status, facility, when custody began, earliest and latest release dates, crimes (up to four), aggregate minimum and maximum sentences, parole hearing dates and results, and post-release supervision dates, are also provided. The Web site also explains why the information is made available:

> Judiciary Law §4 provides that the sittings of every court in the state shall be public and every citizen may freely attend same. Judiciary Law §255 and 255-b generally provide that court records must be kept open to the public and made available upon request.
>
> Similarly, as an agency of state government, the Department must comply with [the] Freedom of Information Law (FOIL) and can only withhold documents that are exempted from disclosure as provided in Public Officers Law §87. Except for information that is specifically made confidential, such as youthful offender records, all conviction and sentence plus other information about offenders presently and previously incarcerated with the Department is considered public information and therefore accessible under FOIL.[350]

d. Montana

The Montana Department of Corrections provides offender information online, and advertises the availability of its entire offender database for a fee.[351] The Montana database includes individuals currently and formerly incarcerated or under supervision by the State. The information provided online includes photographs, personal information (including birthplace, marital status, dependents, citizenship, gender, ethnicity, height, weight, hair and eye color, skin tone, build, whether left- or right-handed, scars, marks, or tattoos, and other physical conditions), and "legal record" information, including docket numbers, offenses, and sentencing information.[352]

State corrections departments generally provide offender information that is limited to persons currently or formerly under State supervision. Many local jurisdictions similarly provide inmate information about offenders who are, or have been, in their jails. For example, while the State of California does not provide statewide offender information to the public on the Internet, the Los Angeles County Sheriff's Department provides information about offenders in its facilities.[353] Entering a first and last name produces personal information (sex, race, date of birth, age, hair and

---

[346] Ibid.

[347] *See* <http://nysdocslookup.docs.state.ny.us/kinqw00> (visited Apr. 5, 2004).

[348] Ibid., at <www.docs.state.ny.us/univinq/fpmsovrv.htm> (visited Apr. 5, 2004).

[349] Ibid.

[350] Ibid.

[351] The Montana Department of Corrections' Offender Web site states that individual offender queries obtained on the site are free, but that the database "is available in its entirety to outside entities for a nominal charge per record plus a $100 cost recovery fee." Montana Department of Corrections, Correctional Offender Network, at <http://app.discoveringmontana.com/conweb/full_list.html> (visited Apr. 5, 2004). Persons interested in purchasing the entire database must sign a database use agreement. Ibid.

[352] Ibid., at <http://app.discoveringmontana.com/conweb> (visited June 29, 2004). Relevant statutes governing availability of the offender information are MCA 2-6-101 et seq. and MCA 44-5.

[353] *See*, generally, <www.lasd.org> (visited June 28, 2004).

eye color, height, and weight), as well as arrest information, court appearance and case information, and release information. Other examples of local jurisdictions that provide offender information include the Shelby County Sheriff's Office in Memphis, Tenn.,[354] and the McCracken County Jail in Kentucky,[355] both of which provide online arrest and other data concerning the individuals held in their respective jails.

Finally, many States and local jurisdictions also provide information concerning whether an offender is in custody through the Victim Information and Notification Everyday (VINE) system. Accessible by telephone, this system was intended to provide a vehicle for crime victims to register with the sponsoring jurisdiction to be notified automatically when an offender is released, transferred, or escapes. Anyone can access the system to obtain offender information, however, even if they do not wish to register to be notified of custody changes. The available information typically includes, at a minimum, the offender's name, date of birth, race, gender, custody status, and where the inmate is being held. At least 30 States make the VINE system accessible via the Internet through a searchable database known as "Vinelink" provided by Appriss.[356]

These databases, and many more like them, clearly provide substantial personal and criminal history information to the public. The number of databases and the efficiency of their use by commercial vendors, while variable from jurisdiction to jurisdiction, is likely to increase.

4. Access to local police department records

Original records of entry into the criminal justice system—colloquially referred to as "police blotters"—contain the first record of an individual's arrest. Police blotters typically include, at a minimum, the name, age, sex, and race of persons arrested, along with citations to alleged offenses. This information, usually organized chronologically and maintained on a local level, has traditionally been publicly available, and remains so today.[357]

By and large, police blotter data are exempted from State statutes that protect criminal history information.[358] Similarly, such data are exempted from the U.S. DOJ regulations designed to protect the confidentiality of criminal history information.[359] In addition, State FOIA statutes commonly make police blotter information expressly subject to open records requirements.[360] However, many statutes require that certain categories of information be kept confidential, such as investigative data, names of victims, Social Security numbers, and the like.[361]

While police blotter information is theoretically available to the public, as a practical matter, in some instances it may not be easy to obtain.[362] The ease of obtaining the information is likely to vary considerably from jurisdiction to jurisdiction. As discussed previously, however, some local jurisdictions make police blotter-type arrest information available in online databases.

B. Regulation of the practices of commercial vendors

The second category of laws that impact the commercial vendor

[354] *See* Shelby County Sheriff's Office Web site at <www.shelbycountyjail.com/scsoweb/injail.htm> (visited June 28, 2004).

[355] *See* McCracken County Jail Current Inmate Listing at <http://mcccj.com/lookup> (visited June 28, 2004).

[356] *See* <www.vinelink.com> (visited June 28, 2004).

[357] *See*, generally, Robert R. Belair, *Original Records of Entry,* Criminal Justice Information Policy series, NCJ 125626 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, November 1990) at pp. 5–11, 16–37.

[358] *See*, *for example,* Mass. Gen. Laws Ann. Ch. 6 § 172 (exempting "police daily logs, arrest registers, or other similar records compiled chronologically, provided that no alphabetical arrestee, suspect, or similar index is available to the public, directly or indirectly"); Hawaii Rev. Stat. Ch. 846-8.

[359] 28 C.F.R. § 20.20(b)(2) (exempts "police blotters maintained by criminal justice agencies, compiled chronologically and required by law or long standing custom to be made public, if such records are organized on a chronological basis.").

[360] *See, for example,*, Cal. Govt. Code § 6254(f); Fla. Stat. Ch. 119.001(3)(c); 5 Ill. Comp. Stat. 160/4a (arrest reports must be made available to the news media); Minn. Stat. § 13.82; R.I. Gen. Laws § 38-2-2(4)(D).

[361] *See, for example,* Fla. Stat. Ch. 119.07(f)(1).

[362] *See, for example,* Reporters' Committee for Freedom of the Press, "Five More States & D.C. Put Open Records Laws to the Test," *The News Media & the Law*, Vol. 24, No. 4 (Fall 2000) available at <www.rcfp.org/news/mag/24-4/foi-fivemore.html> (reporting on surveys in Oklahoma, Maryland, Minnesota, Oklahoma, California, and Iowa) (visited June 28, 2004).

industry consists of statutes that regulate the practices of commercial vendors selling criminal justice information. The principal statute in this area is the Federal Fair Credit Reporting Act (FCRA), which regulates the production of consumer reports, including criminal background checks, by consumer reporting agencies for various permissible purposes, including employee and tenant screening.[363] The primary focus of the FCRA is the commercial vendor (that is, the consumer reporting agency), although the FCRA also imposes some obligations on employers and other users of consumer reports (the FCRA does not, however, apply to end-users who obtain the records directly from a government agency for their own use).

In addition to the Federal statute, many States have adopted their own "mini" FCRA statutes. Both Federal and State consumer reporting laws provide a number of safeguards for individuals, particularly in cases where the report is to be used in whole or in part for an employment determination. In some cases, State laws provide significant additional protections beyond those found in the Federal law.

1. The Federal Fair Credit Reporting Act

The Fair Credit Reporting Act of 1970, as amended, is one of the most comprehensive measures regulating the privacy of personal information in the private sector.[364] Despite the name of the Act, it regulates far more than credit information. The purpose of the FCRA is to promote the accuracy, fairness, and privacy of personal information held and distributed by consumer reporting agencies. Among other things, the FCRA regulates the use of criminal justice information by consumer reporting agencies for employment, credit, and certain other purposes. As noted, its restrictions do not apply to an end-user who obtains criminal justice information directly from government sources, or from a third party that does not fit within the FCRA's definition of a consumer reporting agency.

As defined in the FCRA, consumer reporting agencies are organizations that, for a fee or on a cooperative nonprofit basis, are in the practice of assembling or evaluating personally identifiable information obtained from third parties and bearing upon a consumer's credit worthiness, character, reputation, personal characteristics, or mode of living.[365] This, of course, includes criminal justice information.

Under the FCRA, a consumer reporting agency may provide such information to a party only when the agency has reason to believe the party will use the report for a "permissible purpose" as defined in the FCRA.[366] These purposes include making a determination on credit, employment, insurance underwriting, or otherwise in connection with a legitimate business need in a transaction involving the consumer or pursuant to written instructions of the consumer. Reports can also be provided in connection with firm offers of credit or insurance.[367] A consumer reporting agency's communication of information, which is used, expected to be used, or collected in whole or in part for a permissible purpose, is known by the FCRA-defined term, "consumer report."[368]

The FCRA, which was substantially amended in 2003, includes a wide range of safeguards for consumers, including notice to consumers; consent, including opportunities for opt-in/opt-out; accuracy, relevance, and timeliness standards; confidentiality and use safeguards; security expectations; consumer access and correction rights; content restrictions; and remedies, including administrative sanctions and private rights of action. The Act establishes obligations for consumer reporting agencies as well as for their customers—the end-users of consumer reports. The discussion below highlights those obligations that are particularly relevant to criminal justice information and consumer reports, including background checks that are provided for employment screening purposes.

a. Obligations of consumer reporting agencies under FCRA

Consumer reporting agencies rely upon the representations of their customers concerning the intended permissible purposes for the requested information. Agencies must have a reasonable basis for

[363] Although not obvious from the statute's name, as addressed further in this section, the FCRA and the consumer privacy protections contained within it regulate not only the reporting of credit information, but also the use and reporting of criminal justice information by consumer reporting agencies, which perform much of the background screening that is done for employment and related purposes.

[364] 15 U.S.C. § 1681 et seq.

[365] Ibid., at § 1681a(f).

[366] Ibid., at § 1681b.

[367] Ibid.

[368] Ibid., at § 1681a(d).

this reliance but they do not otherwise have to verify or audit the representation. Accordingly, the FCRA requires the agencies to maintain "reasonable procedures" designed to limit the furnishing of consumer reports to the purposes permitted under the Act; these procedures require prospective users of the information to identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose.[369] The consumer reporting agency must also make a reasonable effort to verify the identity of new prospective users and the intended uses certified by such new users.[370] Finally, in preparing a consumer report, a consumer reporting agency must follow reasonable procedures to ensure maximum possible accuracy of the information included in the report.[371]

Under the FCRA, a consumer report may be furnished for "employment purposes," which is defined to mean "evaluating a consumer for employment, promotion, reassignment or retention as an employee."[372] The definition has been interpreted broadly to include, for example, employers who are: merely considering the possibility of terminating an employee; investigating allegations of workplace wrongdoing against a current employee; hiring independent contractors; or, determining whether a contractor's employee should have a security clearance.[373] At least one court has also approved as an employment purpose a State licensing board's receipt of a consumer report in order to evaluate an applicant for a professional license.[374] An employer may not obtain a consumer report on a former employee, or on someone other than the subject of its decisionmaking, such as the relatives of an employment applicant.[375]

Under the FCRA, a consumer reporting agency that furnishes a consumer report for employment purposes containing public record information—including criminal justice records—which is "likely to have an adverse effect upon a consumer's ability to obtain employment," must either (1) notify the consumer at the time of the report that public record information is being reported to the potential employer, or (2) "maintain strict procedures" to ensure that the information is complete and up to date.[376] Public record information relating to arrests, indictments, convictions, suits, tax liens, and outstanding judgments is considered up to date if the report reflects the public record status of the item as of the time of the report.[377]

In most cases, a consumer reporting agency may not report negative information that is more than 7 years old, including arrest information, although the time limit is 10 years for bankruptcies.[378] The FCRA imposes no time restrictions on the reporting of criminal convictions or on the use of favorable or neutral information.[379] While reports may not include adverse information beyond the specified time periods, reports are not *required* to include adverse information for the entire designated periods.[380] Notably, however, the reporting restrictions do not apply if the consumer report is requested in connection with, among other things, employment of any individual at an annual salary reasonably expected to equal $75,000 or more.[381]

When corresponding with a consumer, a consumer reporting agency must enclose a summary of the consumer's rights under the FCRA.[382] If requested by a consumer, the consumer reporting agency must provide the consumer with a copy of that consumer's file, as well as a listing of everyone who has requested it recently.[383] The cost to the consumer of obtaining the report may

[369]Ibid., at § 1681e(a).

[370]Ibid.

[371]Ibid., at § 1681e(b).

[372]Ibid., at § 1681a(h).

[373]*See* Grimes, FTC Informal Staff Opinion Letter, Oct. 23, 1985; FTC Official Staff Commentary § 604(3)(B) item 1; Isaac, FTC Informal Staff Opinion Letter, Feb. 23, 1998; FTC Official Staff Commentary § 603(h) item 2; Brinckerhoff, FTC Informal Staff Opinion Letter, July 24, 1986.

[374]*Hoke* v. *Retail Credit Corp.,* 521 F.2d 1079 (4th Cir. 1975), *cert. denied*, 423 U.S. 1087 (1976).

[375]FTC Official Staff Commentary, § 604(3)(B) item 2; *Zamora* v. *Valley Federal Savings & Loan Ass'n*, 811 F. 2d 1368 (10th Cir. 1987).

[376]15 U.S.C. § 1681k(a).

[377]Ibid.

[378]Ibid., at § 1681c(a).

[379]Some State statutes are more restrictive.

[380]FTC Official Staff Commentary, 16 C.F.R. § 605.4.

[381]15 U.S.C § 1681c(b)(3). Some State statutes have more restrictive requirements.

[382]15 U.S.C. § 1681g.

[383]Ibid. The agency must identify all end-users who requested the consumer's report for employment purposes during the 2-year period prior to the consumer's request, and those requested for other purposes only during the prior year. Ibid.

not exceed $9, and, in many cases, may be free to the consumer.[384]

Consumers are permitted to request a correction of information they believe to be inaccurate, and the consumer reporting agency must investigate unless the dispute is frivolous.[385] The agency must send a written investigation report to the individual and a copy of the revised report, if changes were made; the consumer may request that corrected reports be sent to recent recipients and, if the dispute is not resolved in the consumer's favor, the consumer has the option of including a brief statement in his or her file, typically for distribution with future reports.[386] A consumer reporting agency must remove or correct unverified or inaccurate information in its files, typically within 30 days after the consumer disputes the information.[387]

Consumers may sue for willful or negligent violations or seek assistance from the U.S. Federal Trade Commission and other Federal agencies responsible for the enforcement of the FCRA.[388]

b. Obligations of end-users under FCRA

An end-user of information obtained from a consumer reporting agency also has obligations under the FCRA. The end-user must, for example, certify to the consumer reporting agency that the end-user has a permissible purpose to obtain the report. The end-user is prohibited from using the report for other purposes. In addition, the end-user must also provide notice to the consumer if it takes an adverse action against the consumer, based in whole or in part on the contents of the consumer report. The adverse action notice must include the name, address, and telephone number of the consumer reporting agency, a statement that the consumer reporting agency did not make the decision to take the adverse action, and a notice of the consumer's right to dispute the accuracy or completeness of any information furnished by the consumer reporting agency.[389]

In the employment context, an employer or potential employer has additional obligations. The employer or potential employer must notify and obtain consent from the employee or applicant before seeking a consumer report from a consumer reporting agency for an employment purpose.[390] A consumer reporting agency may not furnish an end-user with a report for employment purposes unless the end-user first certifies to the agency that (a) it has disclosed to the consumer that a consumer report may be obtained for employment purposes; (b) the consumer has authorized in writing the procurement of the report; and (c) prior to taking any adverse action based in full or in part on the consumer report, the employer will give the consumer a copy of the report along with the summary of the consumer's rights under the FCRA.[391]

In the employment context, "adverse action" includes denial of employment or any employment decision that adversely affects a current or prospective employee, including termination, denial of promotion or job transfer, or even denial of a security clearance for a government contractor's employee.[392] As the above certification obligations indicate, before taking any adverse action in reliance upon information in the consumer report, the end-user must provide the consumer with a copy of the consumer report and the summary of rights.[393] This "pre-adverse action" notice is intended to give the consumer the opportunity to review the report for accuracy and completeness before the employer makes a final decision. In addition to these pre-adverse action disclosures, if an adverse action does occur, based in whole or in part upon information in the consumer report, the employer must still provide the notice of adverse action.

2. State consumer reporting statutes

Approximately one-half of the States have their own fair credit reporting statutes. Many include provisions similar to those in the Federal FCRA, but some are even more restrictive.

State law is fully preempted with respect to certain specified FCRA provisions.[394] In the case of FCRA provisions that are not fully preempted, State law is preempted only to the extent that it is inconsistent with the FCRA.[395] This has been interpreted to mean that State

[384]Ibid., at § 1681j.

[385]Ibid.

[386]Ibid.

[387]Ibid.

[388]Ibid., at §§ 1681n, 1681o, 1681s.

[389]Ibid., at 1681m.

[390]Ibid., at § 1681b.

[391]Ibid.

[392]Ibid., at § 1681a (h) and (k); FTC Official Staff Commentary, § 603(h), item 2.

[393]Ibid.

[394]15 U.S.C. § 1681u.

[395]Ibid.

law is preempted only when compliance with an inconsistent State law would result in violation of the FCRA.[396] In general, there is no inconsistency if the State law is more protective of consumers.[397]

Many State fair credit reporting laws impose obligations on credit reporting agencies and end-users that differ from those imposed by the FCRA without being inconsistent, making compliance with all applicable laws complicated. For example, in at least four States (California, Montana, Nevada, and New Mexico), a consumer reporting agency may not report convictions that are more than 7 years old, even though the FCRA imposes such a time restriction only on the reporting of arrests, and has no limitation on convictions.[398] Also, unlike the FCRA, California, New Mexico, and New York preclude the reporting of arrests that do not result in convictions.[399]

In addition, some States set the employee's expected salary level, which governs the applicability of time limits on reporting arrest information, at levels differing from that set in the FCRA. Whereas the FCRA imposes the 7-year restriction on the reporting of arrest information if the expected salary is less than $75,000, the laws in at least four States impose the 7-year restriction on the reporting of arrests only if the employee or applicant is expected to earn less than $20,000 per year.[400] Unlike the FCRA, these States also impose the 7-year restriction limit on the reporting of convictions if the expected salary is less than $20,000.

Some State laws also impose disclosure requirements that differ from those in the FCRA. For example, in some States, employers must provide employees/applicants with a copy of the consumer report they obtain for employment purposes, regardless of whether they take any adverse action in reliance upon the report.[401] In addition, California requires end-users, including prospective or current employers, to disclose to the consumer any information gathered on the person's character, general reputation, personal characteristics, or mode of living—including criminal justice information—even if the employer itself obtains the information directly without using a consumer reporting agency.[402]

C. Regulation of information that end-users, particularly employers and landlords, can use to make employment and housing decisions

The third category of law, which indirectly impacts the commercial vendor industry, consists of regulation of the ability of end-users, particularly employers and landlords, to consider certain criminal justice information in the course of making decisions that impact the individual.[403] End-users customarily enjoy considerable leeway in making decisions on the basis of criminal justice information, unless there is a specific prohibition in law. Laws in this category include equal employment and fair housing laws at the Federal, State, and local level. Commercial vendors can provide additional value for end-users by providing guidance and by tailoring their reports to account for these laws.

1. Regulation of employers' access to criminal justice information

On the Federal level, Title VII of the Civil Rights Act of 1964[404] prohibits discrimination on the basis of factors such as race, color, sex, religion, and national

[396] *See* FTC Official Staff Commentary, § 622.1.

[397] The FCRA also includes certain specific preemption provisions that override *any* State law that differs from the Federal provision, regardless of its consistency with the FCRA, depending upon when the State law was enacted. *See, for example,* 15 U.S.C. § 1681t(b)(1).

[398] Cal. Civ. Code § 1786.18(a)(7) (California); Mont. Code Ann. § 31-3-112(5) (Montana); Nev. Rev. Stat. 5698C.150(2) (Nevada); N.M. Stat. Ann. § 56-3-6(a)(5) (New Mexico).

[399] Cal. Civ. Code § 1786.18(a)(7) (California); N.M. Stat. Ann. § 56-3-6(a)(5) (New Mexico); N.Y. Bus. Law § 380-j(a)(1) (New York).

[400] Kan. Stat. Ann. §§ 50-704(a)(5) & (b) (Kansas); Md. Code Ann. §§ 14-1203(a)(5) & (b)(3) (Maryland); Mass. Gen. Laws 93 §§ 52(a)(5) & (b)(3) (Massachusetts); N.H. Rev. Stat. Ann. §§ 359-B:5(I)(e) & 5(II)(c) (New Hampshire). New York sets the salary level at $25,000 (N.Y. Gen. Laws §§ 380-j(f)(1)(v) & (j)(f)(1)(iii)), and Texas sets it at $75,000 (Tex. Bus. & Com. Code Ann. §§ 20.05(a)(4) & (b)(3)).

[401] *See, for example,* Cal. Civil Code § 1786.20(a)(2) (California); 20 Ill. Comp. Stat. Ann. 2635/7(A)(1) (Illinois); Minn. Stat. § 13C.03 (Minnesota); Okla. Stat. Tit. 24 § 148 (Oklahoma).

[402] Cal. Civil Code § 1786.53.

[403] The obligations imposed on end-users by the FCRA and corresponding State statutes are discussed in the previous section.

[404] 42 US.C. § 2000e et seq.

origin. The Equal Employment Opportunity Commission (EEOC) and several courts have found that in the employment context, inquiries about arrest records can be a violation of Title VII,[405] although inquiry into and decisions based on convictions are easier to justify. Under Federal law, an employer may consider a potential employee's criminal convictions, and deny employment based on them, provided the employer can establish a legitimate business purpose for doing so.[406] However, in determining whether to consider arrest records in an employment decision, an employer must consider not only the relationship of the charges to the position sought, but also the likelihood that the applicant actually committed the offense charged. In light of this fact, and because some minority groups may be arrested more often than others, courts have found that the use of arrest records in employment decisions has a disproportionate or "disparate" effect on the employment opportunities of the members of these groups. As a result, a blanket policy that an arrest record is an absolute bar to employment (that is, a "zero tolerance" policy), is a violation of Title VII.[407]

More significantly, many State laws expressly prohibit employers from inquiring about a candidate's arrest or conviction record, or severely limit the extent of permissible inquiry, even if there is no evidence that the employer's inquiry will lead to unlawful employment discrimination.[408] In this sense, the State equal employment laws are far more restrictive than the parallel Federal law, because as Title VII has been interpreted and applied, an employer's use of criminal justice information can constitute discrimination, or have a discriminatory impact, *only in certain circumstances*, and the employer can rebut a discrimination allegation by demonstrating that the inquiry is job-related and therefore permissible.

State laws that include blanket prohibitions on employers' inquiries about arrest or conviction records generally do not provide such leeway, however.[409] Several States, such as California, Illinois, Massachusetts, Michigan, New York, and Rhode Island, explicitly prohibit employer inquiries about arrest records.[410] In addition, many States have issued administrative guidance to the same effect: Arizona, Colorado, Kansas, Nevada, New Hampshire, New Jersey, Ohio, South Dakota, Utah, and West Virginia.[411] Other

[405] *See, for example,* 29 C.F.R. § 1607.4(c)(1); *Gregory* v. *Litton Sys.,* 316 F. Supp. 401 (C.D. Cal. 1970), *aff'd as modified*, 472 F.2d 631 (9th Cir. 1972) (fact that an individual suffered a number of arrests without any convictions was not conclusive as to wrongdoing and was irrelevant to work qualifications and, because the mere inquiry into arrest records tends to have a chilling effect on minority job applicants, inquiries about arrests may violate Title VII).

[406] *See, for example, Green* v. *Missouri Pacific Railroad Co.*, 523 F.2d 1290 (8th Cir. 1975); *Carter* v. *Gallagher*, 452 F.2d 315 (8th Cir. 1971), *cert. denied*, 406 U.S. 950 (1972).

[407] *See, for example, Marshall* v. *Klassen*, 1977 US Dist Lexis 17375 (S.D. Ind. 1977); *Green* v. *Missouri Pacific Railroad Co*., 523 F.2d 1290 (8th Cir. 1975). *See also*, *International Brotherhood of Teamsters* v. *United States*, 431 U.S. 324 at 336 n. 15 (1977) (Disparate *impact* results from the use of "employment practices that are facially neutral in their treatment of different groups but that in fact fall more harshly on one group than another and cannot be justified by business necessity; proof of motive is not required.") A decision on the use of an arrest record in making an employment decision must be based upon an individual analysis that considers (1) the nature and gravity of the offense, (2) the time that has passed since the arrest occurred, and (3) the nature of the job held or sought. *Green* v. *Missouri Pacific Railroad Co.*, 549 F.2d 1158, 1160 (8th Cir. 1977).

[408] The EEOC has issued guidance that appears to condone State bans on inquiries, even though the Commission also acknowledges that arrest information can be pertinent to hiring decisions. *See* "Equal Employment Opportunity Commission Policy Guidance on the Consideration of Arrest Records in Employment Decisions Under Title VII 5-6 and 9" (1990).

[409] *See,* generally, Littler Mendelson, *The 2003–2004 National Employer on Compact Disc* (February 2003) at Vol. II, pp. 1105–1130, "Reference Table – State Privacy & Statutory Individual Rights." Hereafter, Littler Mendelson CD.

[410] *See* Cal. Lab. Code § 432.7(a); 775 ILCS 5/2-103; Mass. Gen, Laws ch. 151B 4(9)(ii); Mich. Comp. Laws § 37.2205(a)(1) (prohibits inquiries into misdemeanor arrests only); N.Y. Exec. Law § 296(16); R.I. Gen. Laws § 28-5-7(7).

[411] *See* Labor Policy Association, "Reauthorization of the Fair Credit Reporting Act," Memoranda (Jan. 17, 2003) at p. 20 (hereafter, LPA FCRA memoranda), *citing* Arizona Civil Rights Division's Pre-Employment Guide; Colorado Civil Rights Commission guidelines on pre-employment inquiries; Kansas Human Rights Commission's Guidance on Equal Employment Practices; Nevada Pre-Employment Inquiry Guide; New Hampshire Commission for Human Rights guidelines; New Jersey Guide to Pre-employment Inquiries; Ohio Civil Rights Commission's "A Guide for Application Forms and Interviews"; South Dakota Division of Human Rights Pre-employment Inquiry Guide; Utah Industrial Commis-

States, such as Idaho and Missouri, permit arrest inquiries only if the employer shows business necessity.[412]

Some States are even more restrictive by imposing limits on employers' inquiries into conviction records. For example, the District of Columbia, Alaska, and Ohio prohibit inquiries into convictions more than 10 years old.[413] In addition to limiting inquiries to convictions less than 10 years old, Hawaii permits inquiry into conviction records only if "the conviction record bears a rational relationship to the duties and responsibilities of the position," but such inquiry may take place "only after the prospective employee has received a conditional offer of employment, which may be withdrawn if the prospective employee has a conviction record that bears a rational relationship to the duties and responsibilities of the position."[414] California prohibits inquiries into marijuana convictions more than 2 years old.[415] Massachusetts prohibits inquiries into certain first-time convictions (such as misdemeanor drunkenness, simple assault, speeding, minor traffic violations, or disturbing the peace), as well as other misdemeanor convictions if the conviction, or completion of incarceration resulting from it, occurred 5 or more years earlier, unless the person has been convicted of any offense within 5 years.[416] These restrictions can be significant in light of the penalties that are imposed for violations.[417]

Finally, some States (including Missouri, New Hampshire, New Jersey, Rhode Island, South Dakota, and Utah) allow inquiries into convictions only when the employer proves that such inquiries are job-related.[418] Similarly, New York law provides that an application for employment cannot be denied by reason of the applicant's having previously been convicted of a criminal offense, unless (1) there is a direct relationship between the offense and the employment; or (2) hiring the applicant would involve an unreasonable risk to property or to the safety or welfare of individuals or the public.[419]

2. Regulation of landlords' access to criminal justice information

In the housing context, Federal, State, and local law must also be considered. As noted above, under Federal law, public housing agencies are expressly authorized to obtain criminal justice information with respect to persons applying for public housing.[420] Indeed, public housing agencies (PHAs) and owners of federally assisted housing are expressly required to screen out prospective tenants who have engaged in particular types of criminal activity. For example, they must turn down an applicant who is subject to a lifetime registration requirement under a State sex offender registration program; therefore, they are required to perform "criminal history background checks necessary to determine" whether any household member is subject to such requirements "in the State where the housing is located and in other States where household members are known to have resided."[421]

---

sion, Anti-Discrimination Division Pre-employment Inquiry Guide; and West Virginia Bureau of Employment Programs Guidelines for Pre-Employment Inquiries. Some States make exceptions for particular categories of employers.

[412]Ibid., citing the Idaho Human Rights Commission Pre-employment Inquiry Guide; Missouri Guide to Pre-employment Inquiries.

[413]Ibid., citing Alaska Admin. Code tit. 13 § 68.310(b)(3); District of Columbia Code Ann. § 2-1402.66; Ohio Civil Rights Commission's "A Guide for Application Forms and Interviews."

[414]Haw. Rev. Stat. § 378-2.5; Hawaii Civil Rights Commission Guideline for Pre-Employment Inquiries.

[415]Cal. Lab. Code § 432.8.

[416]Mass. Gen. Laws Ch. 151B § 4(9)(ii).

[417]For example, California imposes a $200 fine for each violation (a minimum of $500 for an intentional violation). Cal. Labor Code § 432.7(c). These penalties can add up if an employer were to include an improper inquiry on hundreds of employment applications and a class action were to be brought on behalf of all applicants.

[418]*See* LPA FCRA memoranda, *supra* note 411, at p. 20, citing Missouri Guide to Pre-employment Inquiries; New Hampshire Commission for Human Rights guidelines; New Jersey Guide to Pre-employment Inquiries; Rhode Island Commission for Human Rights Guidelines; South Dakota Division of Human Rights Pre-employment Inquiry Guide; and Utah Industrial Commission, Anti-Discrimination Division Pre-employment Inquiry Guide.

[419]*See* N.Y. Exec. Law § 296(15) and Corr. Law § 752

[420]*See* 42 U.S.C. § 1437d(q).

[421]24 CFR § 882.518(a)2; *see also* 24 CFR §§ 5.856, 960.204. PHAs must also deny admission to an applicant who has "ever been convicted of drug-related criminal activity for manufacture or production of methamphetamine on the premises of federally assisted housing" or who has been evicted from public housing within the previous 3 years for drug-

Public housing agencies are authorized to obtain criminal history record information from the National Crime Information Center (NCIC), FBI, State and local police departments, and other law enforcement agencies.[422] But guidance from the U.S. Department of Housing and Urban Development (HUD) has made clear that they are not required to use such sources, and that they can contract out their background screening obligations.[423] Once a PHA or owner obtains criminal history records for screening purposes, they must establish and implement a records management system that will maintain the confidentiality of the records.[424] In addition, before a conviction can be used as a basis for denying admission, enforcing a lease, or evicting a tenant, the subject must be given an opportunity to dispute the accuracy and relevance of the criminal history information.[425]

Under the HUD regulations, PHAs are required to establish policies, within certain guidelines, to govern how they will screen out applicants who have engaged in criminal activities, but they have substantial discretion in setting such policies. Thus, for example, in screening family behavior and suitability for tenancy, the PHA may consider "all relevant information," which may include, *inter alia*, "a history of criminal activity involving crimes of physical violence to persons or property and other criminal acts which would adversely affect the health, safety, or welfare of other tenants."[426] The tenant selection criteria to be established and information to be considered must be "reasonably related to individual attributes and behavior of an applicant," and not related to "those which may be imputed to a particular group or category of persons of which an applicant may be a member."[427] If unfavorable information is obtained about an applicant, "consideration shall be given to the time, nature, and extent of the applicant's conduct" and to other factors that could point to favorable future conduct, such as evidence of rehabilitation or participation in appropriate programs.[428]

Even outside the context of federally assisted or public housing where criminal history screening is affirmatively required, there is little to discourage landlords from using criminal history information in tenant screening. Unlike the situation faced by employers, Federal fair housing law does not preclude the use of criminal history information in making housing-related decisions, since persons with criminal records do not constitute a legally protected class.[429] Indeed, the Fair Housing Act explicitly provides that a dwelling need not be made available "to an individual whose tenancy would constitute a direct threat to the health or safety of other individuals or whose tenancy would result in substantial physical damage to the property of others."[430]

As a general matter, State fair housing laws also do not include criminal record status as a suspect category on which claims of housing discrimination may be based. For example, the California Fair Employment and Housing Act recognizes discrimination only on

---

related criminal activity. *See* 24 CFR §§ 5.854, 882.518, 960.204.

[422]The NCIC, police departments, and other law enforcement agencies are authorized to give PHAs information regarding "criminal conviction records" of adult applicants "for purposes of applicant screening, lease enforcement and eviction." 42 USC 1437d(q)(1)(A). To obtain access to such records, the PHA must require applicant families to submit a consent form signed by each adult household member. *See, for example,* 24 CFR 5.903(b).

[423]*See, for example,* Department of Housing and Urban Development, "Screening and Eviction for Drug Abuse and Other Criminal Activity: Discussion of Final Rule," 66 *Federal Register* 28776 et seq. (May 24, 2001) at 28776 ("although this rule provides a mechanism for obtaining access to criminal records, HUD recognizes that many PHAs and owners may now use other means of obtaining criminal records and may continue to use these other means … However, HUD cautions PHAs and owners to handle any information obtained about criminal records in accordance with applicable State and Federal privacy laws and with the provisions of the consent forms signed by the applicants."

[424]*See, for example,* 24 CFR § 5.903(g).

[425]*See, for example,* 24 CFR § 5.903(f).

[426]*See, for example,* 24 CFR § 960.205(b)(3).

[427]24 CFR § 960.203(a)

[428]Ibid.

[429]Title VIII of the Civil Rights Act of 1968 (Fair Housing Act), as amended, prohibits discrimination in the sale or rental of dwellings based on race, color, national origin, religion, sex, familial status (including children under the age of 18 living with parents of legal custodians, pregnant women, and people securing custody of children under the age of 18), and handicap (disability). 42 U.S.C. § 3604. Although the categories of unlawful discrimination identified in the Fair Housing Act do not refer to criminal arrest or conviction status, in light of the disparate impact analysis that has been adopted in the employment context, it is possible that the Fair Housing Act could be interpreted to provide similar protections.

[430]42 U.S.C. § 3604(f)(9).

the basis of race, color, religion, marital status, national origin, ancestry, familial status, disability of the person, sexual orientation, and age.[431] Similarly, the New York Human Rights Law identifies bases of unlawful discrimination in housing to include only race, color, creed, national origin, sexual orientation, military status, sex, age, disability, marital status, or familial status, although as noted above, employment may not be denied because of a conviction record unless there is a relationship between the offense and the employment.[432] In Wisconsin, housing discrimination is prohibited based on sex, race, color, sexual orientation, disability, religion, national origin, marital status, family status, lawful source of income, age, or ancestry.[433] Even in the District of Columbia, which has a broad Human Rights Act, housing may not be denied "for a discriminatory reason based on the actual or perceived: race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, familial status, family responsibilities, disability, matriculation, political affiliation, source of income, or place of residence or business of any individual."[434]

Landlords must also comply with local fair housing ordinances, however. Some local jurisdictions have included refusals to rent to persons with records of criminal convictions or arrests among categories of "discrimination" in their fair housing ordinances. For example, in Wisconsin, the Dane County Fair Housing Ordinance provides that unlawful housing discrimination includes discrimination on the basis of arrest or conviction record, in addition to race, gender, age, religion, color, national origin, ancestry, marital status, family status, mental illness, physical condition, appearance, lawful source of income, student status, sexual orientation, military discharge status, or political beliefs.[435] Similarly, the cities of Champaign and Urbana, Ill., prohibit discrimination based on prior arrest or conviction record, as well as personal appearance, sexual preference, matriculation, political affiliation, or source of income.[436] In contrast, New York City's Human Rights Law does not include such a protected class, although it does preclude discrimination based on actual or perceived gender identity, alienage or citizenship status, age, and lawful occupation, among others.[437] Similarly, while San Francisco ordinances prohibit discrimination in housing and public accommodations based on race, religion, color, ancestry, age, sex, sexual orientation, gender identity, disability or AIDS/HIV status, familial status, source of income, weight, height, or place of birth, persons with arrest or conviction records are not protected.[438]

D. Negligence doctrines that encourage employers and landlords to obtain criminal justice record information

The judicial doctrines of negligence constitute an additional incentive for users, such as employers and landlords, to conduct criminal background checks in order to minimize potential liability that may occur in the event that an employee or tenant harms a coworker, customer, tenant, or member of the public.

1. Negligent hiring and retention

Courts in the majority of States recognize the theory of negligent hiring, under which employers may be held liable for actions of their employees that are outside the scope of their employment.[439] The doctrine applies in cases where an employer fails to exercise proper care in selecting and

[431] *See* Cal. Gov. Code § 12955 et seq.

[432] *See* N.Y. Exec. Law, Art. 15, § 296(5); N.Y. Corr. Law, Art. 23-a.

[433] Wisc. Stat. § 106.50.

[434] D.C. Code § 2-1402-21 (a).

[435] Dane County Ordinances, § 31.02. The City of Appleton, Wisc., also recognizes persons with arrest or conviction records as a protected class. *See* Metropolitan Milwaukee Fair Housing Council Web site at <www.fairhousingwisconsin.com> (visited Apr. 6, 2004).

[436] *See* Community of Urbana-Champaign Cooperative Housing, "COUCH and Fair Housing Laws" (Nov. 12, 2002) available at <www.couch.coop/library/fair-housing.html> (visited Apr. 6, 2004).

[437] *See, for example,* the New York City Commission on Human Rights Web site, at <www.nyc.gov/html/cchr/html/housing.html> (visited Apr. 6, 2004).

[438] *See* the San Francisco Human Rights Commission Fair Housing and Public Accommodations Web site at <www.sfgov.org/site/sfhumanrights_page.asp?id=5915> (visited Apr. 6, 2004).

[439] *See,* generally, Littler Mendelson CD, *supra* note 409, at Vol. I §§ 233–235; Vol. III § 257; Robert Hunter, "Past as Prologue: Assessing Job Candidates," Security Management Online (March 2002) available at <www.securitymanagement.com/library/001244.html> (visited Apr. 6, 2004).

retaining employees; that is, the employer knew, or should have known, that an employee poses a threat to coworkers, customers, or the general public. Under this doctrine, an employer may be liable for damages caused by that employee.

The tort of negligent hiring is not based on principles of vicarious liability, such as those covered by the doctrine of *respondeat superior*, under which an employer is held responsible for the employee's acts within the scope of his or her duties, or in furtherance of the employer's interests. Instead, "negligent hiring is a doctrine of primary liability; the employer is principally liable for negligently placing an unfit person in an employment situation involving an unreasonable risk of harm to others."[440] Thus, in negligent hiring cases, "the ultimate question of liability to be decided is 'whether it was reasonable for an employer to permit an employee to perform his job in light of information about the employee which [the] employer should have known.'"[441] Under a negligent hiring theory, the employer's liability extends to an employee's intentional torts and crimes, and other acts outside the scope of the employee's job responsibilities.[442] In many jurisdictions, the negligent hiring theory has been expanded to include the related torts of negligent retention and negligent supervision, which have similar elements, but arise at different points in the employment relationship.[443]

Some States recognize a rebuttable presumption of "due care" in hiring.[444] Even with such a presumption, however, conducting a thorough pre-employment background check has become increasingly important in protecting an employer from potential liability for negligent hiring.[445]

---

[440] *J.* v. *Victory Tabernacle Baptist Church*, 372 S.E.2d 391, 394 (Va. 1988), citing Note, Minnesota Developments – Employer Liability for the Criminal Acts of Employees Under Negligent Hiring Theory: *Pontiacs* v. *K.M.S. Investment*, 68 *Minn. L. Rev.* 1303, 1306–07 (1984) (confirms Virginia's recognition of tort of negligent hiring; church knew or should have known that employee, who sexually assaulted a young girl, had been convicted of similar crime and was on probation).

[441] *Brown* v. *Zaveri*, 164 F.Supp.2d 1354, 1360 (S.D. Fla. 2001) (quoting from *Gillis* v. *Sports Auth., Inc.*, 123 F. Supp.2d 611, 617 (S.D. Fla. 2000) (under Florida law, employer is liable for negligent hiring/retention only when the employer "has somehow been responsible for bringing a third person into contact with an employee whom the employer knows or should have known is predisposed to committing a wrong under circumstances that create an opportunity of enticement to commit such a wrong"; negligent hiring claim dismissed because McDonald's had no actual or constructive knowledge that manager would assault a customer)).

[442] Some States have held that negligent hiring actions cannot be brought against employers for the acts of independent contractors. *See, for example, Camargo* v. *Tjaarda Dairy*, 25 Cal. 4th 1235, 1238 (2001); *Kahrs* v. *Conley*, 729 N.E.2d 191 (Ind. Ct. App. 2000) (court confirmed long-standing rule that principal is not liable for negligence of an independent contractor, but recognized five exceptions to that general rule: if the work is intrinsically dangerous, will create a nuisance, will probably cause injury without due precautions, is illegal, or if the principal is, by law, charged with performing the specific duty); *Giles* v. *Shell Oil Corp.*, 487 A.2d 610 (D.C. 1985).

[443] *See, for example, Retherford* v. *AT&T Communications of the Mountain States, Inc.,* 844 P.2d 949, 973 n. 15 (Utah 1992) (tort of negligent employment encompasses negligent hiring, negligent supervision, and negligent retention). *See also Yunker* v. *Honeywell,* 496 N.W.2d 419, 423 (Minn. Ct. App. 1993) (doctrines of negligent hiring and negligent retention are distinct theories of recovery; difference focuses on when employer was on notice that an employee posed a threat and failed to take steps to ensure safety of third parties). As a practical matter, the use of background checks to avoid potential negligent retention liability is much less widespread than in connection with initial hiring, as there is great variability in the frequency with which employers perform background checks of existing employees, particularly in the absence of a specific precipitating event. *See*, generally, Littler Mendelson CD, *supra* note 409, at Vol. I §§ 233–235, Vol. III § 257.

[444] *See, for example,* Fla. Stat. Ch. 768.096 (1999) (employer presumed not to have been negligent in hiring if, before hiring the employee, the employer conducted a background investigation which did not reveal information that reasonably demonstrated unsuitability); *Evans* v. *Morsell*, 395 A.2d 480 (Md. 1978).

[445] *See for example, Doe* v. *Garcia,* 961 P.2d 1181 (Idaho 1998) (hospital employee molested a patient; if hospital had inquired of previous employer, his personnel file would have shown previous similar offense); *Oakley* v. *Flor-Shin Inc.*, 964 S.W.2d 438 (Ky. Ct. App. 1998) (evidence that employer knew, or would have known if it had conducted a criminal background check as per its established policy, of employee's past criminal record, presented issue of fact on negligent hiring theory); *Kladstrup* v. *Westfall Health Care Center, Inc.*, 701 N.Y.S.2d 808, 811 (Sup.Ct. N.Y. 1999) (nature of duties of nurse's aide oblige employer "to make an in-depth inquiry to assure that an applicant … does not have a history of sexual misconduct"); *Kelley* v. *Baker Protective Servs., Inc.,* 401 S.E.2d 585 (Ga. Ct. App. 1991) (fact that background check performed on employee revealed no convictions or propensities for criminal behavior supported sum-

In order to prevail on a negligent hiring claim, the plaintiff must prove that the employer knew or should have known of the employee's dangerous propensities and that the employer's negligence caused the plaintiff's damages. Cases have held that a plaintiff can satisfy the first requirement by showing evidence exists that would have put the employer on notice, or that a more thorough background check would have revealed pertinent information.[446] Conversely, courts have also held that performance of an adequate or industry-accepted background check can insulate an employer from a negligent hiring claim.[447] In general, the decision concerning the need for, and adequacy of, a background check hinges upon the type of position at issue. If the position is likely to involve frequent contact with the public, the bar is likely to be set higher, although depending upon the type of position at issue, an adequate background check does not always require investigation of criminal history records.[448]

Many examples of egregious situations have resulted in employers' liability. For example, in *T.W.* v. *City of N.Y.*, a community center custodian sexually assaulted a young girl. The custodian had stated on his employment application that he had a criminal conviction, but the employer did not investigate the applicant's criminal history, which included armed robbery, assault, theft, burglary, and possession of a controlled substance. The court held that because the employer knew that the applicant had a criminal background, it had a duty to investigate further.[449]

Similarly, a jury awarded $3 million to a 55-year-old mentally handicapped woman who had been raped by a bus driver. The driver had been hired, without a criminal background check, to transport handicapped persons. It turned out that he had been previously convicted of robbery, reckless driving, concealment of a firearm, and possession of marijuana. The victim based her claims against the bus company on several theories, including negligent hiring, arguing that the bus company should have performed a criminal background check on the driver. The U.S. Court of Appeals

---

mary judgment for employer on negligent hiring claim); *Burnett* v. *C.B.A. Sec. Serv.,* 820 P.2d 750 (Nev. 1991) (background check performed by employer and sheriff's department revealed no indication that employer would commit offense); *Welsh Mfg.* v. *Pinkerton's, Inc.* 474 A.2d 436 at 441 (R.I. 1984) (security service employee assisted thieves in robbery; court found that "background checks in these circumstances should seek relevant information that might not otherwise be uncovered. When an employee is being hired for a sensitive occupation, mere lack of negative evidence may not be sufficient to discharge the obligation of reasonable care.").

[446]*See, for example, Murray* v. *Research Found. of State Univ. of N.Y.,* 707 N.Y.S. 2d 816 (N.Y. Sup. Ct. 2000), *aff'd* 283 A.D.2d 995 (N.Y. App. Div. 4th Dept. 2001) (necessary element of a cause of action for negligent hiring is that employer knew or should have known of employee's propensity for the conduct that caused injury; proof can include evidence that more thorough background check would have uncovered such information); *Evan F.,* 8 Cal. App. 4th 828 (1992) (in California, employer can be held liable for negligent hiring if he knows the employee is unfit, or has reason to believe employee is unfit, or fails to use reasonable care to discover the employee's unfitness before hiring him); *Abbot* v. *Payne*, 457 So. 2d 1156 (Fla. Dist. Ct. App. 1984) (company found liable for negligent hiring because it failed to inquire into the past employment or references of an employee who physically assaulted a customer); *Ponticas* v. *K.M.S. Inv.,* 331 N.W.2d 907 (Minn. 1983) (employer liable for hiring a resident apartment manager with a violent criminal background who raped a tenant living in the apartment); *Gaines* v. *Monsanto Co.,* 655 S.W.2d 568 (Mo. Ct. App. 1983) (parents of murdered woman sufficiently alleged a cause of action for negligent hiring or retention of a mail clerk, a convicted rapist).

[447]*See, for example, C.C.* v. *Roadrunner Trucking, Inc.*, 823 F.Supp. 913 (D.Utah 1993), affirming Magistrate's Decision reported at 1993 U.S. Dist. Lexis 7251(background check of type usually performed in trucking industry was performed and deemed adequate, in case in which truck driver raped hitchhiker); *Gay* v. *United States*, 739 F.Supp. 275 (D. Md. 1990) (employer had conducted thorough background check; assault was unpredictable, out of character, and could not reasonably have been anticipated or guarded against by employer); *Connes* v. *Molalla Transport System, Inc.*, 831 P.2d 1316 (Colo. 1992); *Burnett* v. *C.B.A. Sec. Serv.*, 820 P.2d 750 (Nev. 1991).

[448]*See, for example, Connes* v. *Molalla Transport System, Inc.,* 831 P.2d 1316, 1320-23 (Colo. 1992) (trucking company had no duty to conduct investigation of driver's criminal history because level of required investigation depends on type of work and anticipated potential contact with public); *Furniture Co.* v. *Harrison*, 583 So.2d 744, 750 (Fla. Dist. Ct. App. 1991) (employer's responsibility to investigate employee's background is defined by the type of work to be done); *Ponticas* v. *K.M.S. Inv.*, 331 N.W.2d 907, 913 (Minn. 1983) (employer's liability for negligent hiring is determined by the totality of circumstances surrounding hiring and whether employer exercised reasonable care). *See, generally,* Littler Mendelson CD, *supra* note 409, at Vol. I §§ 233–235; Vol. III § 257.

[449]*T.W.* v. *City of N.Y.*, 286 A.D.2d 243 (N.Y. App. Div. 1st Dept., September 2001).

for the Fourth Circuit upheld the verdict and affirmed the judgment.[450]

In light of the rising number of statutorily required criminal background checks, and the increasing accessibility of criminal justice information to employers of all types, it is not surprising that the public, as well as courts, have concluded, in more and more circumstances, that it is "reasonable" to expect employers to review the criminal background of job applicants. Consequently, the incentive for employers to do so, if only to protect themselves from potential liability, has also increased.

The extent of this "incentive," however, can be overstated. Most successful negligent hiring claims involve employees with unsupervised access to vulnerable populations (children, the elderly) or sensitive venues. Even today, most employers are unlikely to ever be confronted with a negligent hiring judicial challenge.

2. Negligence theories applicable to claims against landlords

There does not appear to be a definitive legal doctrine of "negligent leasing" similar in nature to the more well-established doctrine of negligent hiring. Nonetheless, under certain circumstances, such a claim could succeed under general theories of landlord liability.

It is well established that as a general matter, a landlord has no duty to protect a tenant from the criminal acts of a third person. A landlord is not an insurer, and cannot be held liable for the occurrence of, or resulting damages from, unforeseeable events such as such criminal acts. A landlord does have a duty, however, to provide habitable premises. If a landlord retains control over the security and safety of the leased premises, the landlord has a duty to provide *secure* premises (for example, secure common areas in an apartment complex) by taking reasonable precautions to provide tenants with reasonable security in response to foreseeable dangers.

"Premises liability," a special form of negligence applicable to landlords, can arise if the landlord fails to use ordinary care to reduce or eliminate an unreasonable risk of harm created by a premises condition of which the landlord is, or reasonably should have been, aware.[451] The existence of the landlord's duty depends upon the foreseeability of the harm. Foreseeability, in turn, is based upon whether a reasonably prudent person would have anticipated that an injury was likely to result from the performance or nonperformance of the act.[452]

Thus, as a general matter, under a "premises liability" theory, a landlord could be held liable for negligence if he had reason to know that a crime was likely to be committed against a tenant, failed to take reasonable precautions to prevent such an act (for example, by providing reasonable security or taking other actions), and such failure was the proximate cause of harm to a tenant. Precedent addressing this and similar theories suggests, however, that a plaintiff in such a case would have to meet a high threshold of proof.[453]

If a landlord were to make representations concerning the security he would provide to tenants—perhaps by advertising that he conducts criminal background checks of all tenants or that he will not rent to persons with criminal records—and then the landlord negligently implemented such measures (for example, by failing to perform background checks or failing to take reasonable precautions in light of the results of such checks), one could make a credible argument for liability under a general negligence theory, such as that which under-

[450] *"Beverly," by her Guardian John Doe* v. *Diamond Transportation Services,* 1999 U.S.App.Lexis 11136 (4th Cir. 1999). *See also Read* v. *The Scott Fetzer Co.,* 990 S.W.2d 732 (Tex. 1998) (upholding $160,000 damage award against vacuum cleaner company and its distributor for failure to verify references or conduct criminal background check of door-to-door salesman who raped a customer in her home).

[451] *See, for example,* discussion in *Urena* v. *Western Investments Corp.,* 2003 Tex. App. Lexis 7152 (Ct. App., 1st Dist., 2003), citing *Timberwalk Apartments Partners, Inc.* v. *Cain*, 972 S.W.2d 749 (Tex. 1998).

[452] *See, for example, Johnson* v. *Spectrum of Supportive Services,* 2003 Ohio 4404 (2003)*; Urena* v. *Western Investments Corp.,* 2003 Tex. App. Lexis 7152 (Ct. App., 1st Dist., 2003); *Saelzler* v. *Advanced Group 400*, 225 Cal. 4th 763 (2001); *Mason* v. *U.E.S.S. Leasing Corp.*, 96 N.Y.2d 875 (N.Y. App. 2001); *Valencia* v. *Michaud*, 79 Cal. App. 4th 741 (Cal. App. 2000 (*unpublished, and not citable); Estate of J. Hough* v. *Estate of W. Hough*, 205 W. Va. 537 (1999); *Goode* v. *St. Stephens United Methodist Church*, 329 S.C. 433 (1997); Taylor W. and Taylor J., "A Plaintiff's Approach to the Preparation of Premises Liability Cases Based on the Criminal Acts of Third Persons,"*53 J. Mo. B. 98* (Mar/Apr. 1997).

[453] *See, for example, Saelzler* v. *Advanced Group 400*, 225 Cal. 4th 763 (2001), and other cases cited in this section.

lies the negligent hiring doctrine.[454]

This suggests that if criminal background checks are performed as part of a landlord's tenant screening process, in order to avoid potential liability under a premises liability or general negligence theory, landlords should take reasonable and appropriate actions and precautions in response to the results of such checks.

E. Self-regulatory efforts of commercial information vendors

Self-regulatory efforts taken by commercial information vendors are also relevant. In 1997, for example, a number of major players in the commercial information industry formed the Individual Reference Services Group (IRSG) to regulate the industry's use and dissemination of personal data, including criminal justice information, through a set of self-regulatory principles agreed to by member companies (IRSG Principles).[455] The IRSG Principles operate on the premise that public record information, including criminal justice information, is "usable without restriction unless legally prohibited."[456] The Principles, however, do require companies to (a) make available information about the nature and sources of public record information in their databases, and (b) either correct inaccurate information or direct individuals to the source of the information.[457] The organization announced its dissolution on September 6, 2001, citing implications of the Federal Gramm-Leach-Bliley financial privacy law. Nonetheless, some companies continue to observe the Principles as a standard of good practice.

In January 2003, a new industry organization—the National Association of Professional Background Screeners (NAPBS)—was formed to "represent the interest of companies offering employment and background screening."[458] According to its mission statement, NAPBS exists "to promote ethical business practices, promote compliance with the Fair Credit Reporting Act and foster awareness of issues related to consumer protection and privacy rights within the background screening industry."[459] Among other things, NAPBS intends to provide relevant programs and training to empower its membership "to better serve clients and set standards within the background screening industry."[460]

The NAPBS has formed several committees, including one to focus on establishing an ethics board; the other to provide practical information on the FCRA and form a body of best practices for all members."[461] The organization has adopted a Code of Conduct which, among other things, provides that employees will "perform professional duties in accordance with the law and the highest moral principles," "safeguard confidential information and exercise due care to prevent its improper disclosure," and "avoid injuring the professional reputation or practice of colleagues, clients or employers."[462] The explanations that accompany the NAPBS Code of Conduct state that individuals shall "not knowingly release misleading information nor encourage or otherwise participate in the release of such information."[463]

[454] *See* discussion in *Urena* v. *Western Investments Corp.,* 2003 Tex. App. Lexis 7152 (Ct. App., 1st Dist., 2003) *citing Timberwalk Apartments Partners, Inc.* v. *Cain*, 872 S.W.2d 749 (Tex. 1998).

[455] Available at <www.irsg.org> (site undergoing redesign).

[456] Individual Reference Services Group, "Principles," Principle IV, available at <www.irsg.org.html/industry_principles_principles.htm> (site undergoing redesign).

[457] Ibid., at Principles III and IX.

[458] NAPBS Web site, available at <www.napbs.com/jointoday/invitation.htm> (visited Apr. 6, 2004).

[459] Ibid.

[460] Ibid.

[461] Ibid., at <www.napbs.com/generalinfo/committee.htm> (visited Apr. 6, 2004).

[462] Ibid., at <www.napbs.com/jointoday/conduct.htm> (visited Apr. 6, 2004).

[463] Ibid.

Part III. Criminal justice record information, commercial vendors, and the development of public policy

A. Introduction

Consider the following marketing pitch:

> American businessmen are faced with a grave problem … Our working forces include more than a few radicals, socialists, revolutionaries, Communists and trouble-makers of all sorts. The colleges and schools are educating and training thousands more who will soon be seeking employment. The hiring and training cost to industry for individual workers run into the many thousands of dollars. Before they are employed, their educational and professional backgrounds are screened most carefully. On the other hand, little, if anything, is done to determine their philosophy of life. In many cases this is of paramount importance.
>
> *****
>
> Our files are the most reliable, comprehensive and complete and second only to those of the FBI which, of course, are not available to you…
>
> We can supply you with all the data regarding your people that you may deem advisable …
>
> My office will be glad to send a representative at your request to go into this delicate matter at greater length.[464]

Was this pitch for background checking made in the days immediately following the terrorist attacks of September 11, 2001? Quite the contrary. In fact, it comes from a data management company brochure published in the late 1960s.

It is frequently assumed that the commercial sale of criminal history information (and other personally identifiable public record and publicly available information) is a recent phenomenon. In fact, more than 30 years ago, R. L. Polk testified before Congress that it maintained information on "200 million names in its marketing services division."[465] Actually, R. L. Polk had been compiling and selling a city directory since the early part of the 20th century. Throughout the 20th century, the Polk City Directory, containing the name, address (rent or own), marital status, occupation, place of employment, and telephone number for virtually every adult American, was the Bible for backgrounding and direct marketing.[466]

Commercial information vendors have been collecting, maintaining, and disseminating criminal justice record information obtained from court records and other public record repositories for at least 50 years (newspapers have been collecting, maintaining, and disseminating this same information far longer).

What's different today? Most of the important differences are matters of scale: more criminal justice information is collected and maintained; more customers are served for more purposes; the information is more accurate, complete, and reliable; and the information is far more apt to be combined with other sources of public record and publicly available information to create a more or less complete personal profile.

In Part III, we look at several important public policy questions:

- **Regulation.** Should the information practices of commercial vendors, courts, State repositories, and corrections departments all be subject to the same rules?
- **Privacy.** Should the Fair Credit Reporting Act (FCRA) be amended to impose obligations on all end-users of criminal justice record

[464] C. Pyle, "Uncle Sam is Watching You," at 57–58, 1971, as cited in "Commercial Information Brokers," 4 *Col. Hum. R. L. Rev*. at pp. 217–218 (Winter 1972).

[465] Hearings on H.R. 2730 before the Subcommittee on Postal Operations of the House Committee on Post Office and Civil Service, 91st Congress, second session at p. 69 (1970).

[466] *See* Hearings on H.R. 2730, at p. 56.

information? Should the FCRA be amended so that it reaches all commercial criminal justice record information products?

- **Relevancy.** Are there relevancy considerations in the collection, use, and dissemination of criminal justice record information? If so, who determines what is relevant? Is criminal justice record information relevant to antiterrorism efforts? Should public policy pivot on whether the information in question is arrest information or conviction information?
- **Reintegration.** Each year, approximately 650,000 offenders are released from incarceration. If commercial vendors retain criminal justice record information indefinitely (and make this information available indefinitely), does this frustrate efforts to reintegrate these offenders into society?
- **Biometrics.** Should commercial vendors be permitted, encouraged, or required to use a biometric (presumably a fingerprint) when identifying individuals who are subject to criminal background checks and when matching a criminal justice record to an individual?
- **Data Quality.** If (and this is very much a question) commercial vendor criminal justice record checks suffer from incompleteness, inaccuracy, or staleness, what, if anything, should be done about this from a public policy standpoint?
- **Profiling.** When commercial vendors combine criminal justice data with other personal data to create "profiles," what are the public safety and risk management benefits and what are the privacy threats? Should public policy be developed to address these issues?

B. Should State central repositories, courts, and commercial vendors be subject to the same rules?

This question begs a key public policy question: Does it really make any sense that different privacy protections apply when the exact same information is held by different parties? Specifically, does it make sense that when commercial vendors communicate criminal history data to employers, the protections in the FCRA apply; but, when employers obtain these data directly from courts or law enforcement, and do so for the very same purpose, none of these protections apply?

The BJS/SEARCH National Task Force on Privacy, Technology, and Criminal Justice recommended the development of a "new generation" of confidentiality and disclosure law and policy for criminal justice record information. This new generation of law and policy would take into account—

- the type of information (for example, whether it is conviction or arrest information)
- the extent to which the database contains other types of criminal justice information
- whether other sensitive personal information is maintained with the criminal justice information (for example, medical or financial information)
- the purpose of the intended use of the information.

The Privacy Task Force rejected basing law and policy on the identity of the source or the identity of the party managing the information.[467]

The National Task Force on the Commercial Sale of Criminal Justice Record Information reached a parallel, but more specific, conclusion. The protections and requirements in the FCRA should apply, regardless of whether employers and other users obtain criminal history data from commercial vendors or directly from courts or law enforcement.

1. Systems emerged to meet different needs

It is difficult to understand the Nation's current "stovepipe" system of regulating criminal justice record information (one set of information privacy rules for State central repositories, a second set for the courts, and a third set for commercial vendors) without a historical context.[468]

For many centuries in the United States, as in England, court records have been public by both tradition and law.[469] As a public

[467]Privacy Task Force report, *supra* 106, at p. 73.

[468]Indeed, there is really a fourth set of rules applicable to the media and its acquisition, maintenance, use, and disclosure of criminal history record information.

[469]*Houston Chronicle Publishing Co*. v. *City of Houston* 531 SW 2d 177, 186 (Court of Civil Appeals, Texas 1975), "The press and the public have a constitutional right of access to information concerning crime in the community and to information relating to the activities of law enforcement agencies." On the other

policy matter, access to court records—particularly criminal court records—has been seen as a protection against secret arrests and secret "star chamber" proceedings. Furthermore, access to these records has been seen as a vehicle for effective oversight of the courts and assurance that individuals/defendants receive the benefit of appropriate constitutional rights. The downside of open access to court records is the threat to privacy, but many courts that have looked at this issue have taken comfort from the fact that a court record is incomplete and thus presents only a modest risk to privacy interests.[470]

By contrast, repository records, particularly as they were first developed, were created for the purpose of providing complete and comprehensive information to criminal justice agencies—for law enforcement investigative purposes, for prosecution purposes, and occasionally for sentencing purposes. Because repository records provided a more or less complete picture of an individual's criminal history, they posed a significant privacy risk.[471]

2. Vendor systems and regulatory controls

In a very real sense, commercial vendor services customarily merely extended or amplified court record systems. In recent years, this has been supplemented with corrections information and some repository information where permitted by law. Vendors obtain records from the courts that are entirely public and could, theoretically, be obtained directly from the courts by the end-user. Commercial vendors obtain these records from numerous courts; vet the information for accuracy; verify the individual's identity; update the information; and, in some cases, append other information about the record subject (such as educational records, driving records, and other public records). All of this, of course, could be done by the end-user (and without, therefore, triggering the various privacy protections and restrictions afforded by the FCRA). Many end-users, however, do not have the resources to obtain and assemble this information and find it more convenient and economical to outsource these tasks to commercial vendors.

Today, when end-users obtain criminal history data directly from courts or repositories, some accountability and privacy protection is provided through a patchwork of State-based employment law. In some States, for example, employers are not permitted to base an employment decision, for example, on arrest-only information. The FCRA also imposes some obligations on end-users, particularly those that obtain reports for employment purposes. The Task Force concluded, however, that, where commercial vendors' acquisition, use, and disclosure of criminal justice record information is subject to the FCRA, more accountability and privacy protection applies than when the information is provided to end-users directly by repositories or courts.

Also, under the FCRA, the Federal Trade Commission and State attorneys general can bring enforcement actions for FCRA violations. In addition, aggrieved record subjects may bring private rights of action against the commercial vendor to recover damages. Further, in certain situations, such as when an individual knowingly and willfully obtains information from a consumer reporting agency under false pretenses, criminal penalties are available. Moreover, as noted, most States have also adopted their own version of the FCRA, which may provide additional remedies and protections.

3. Is a unified regulatory system desirable or even possible?

A central public policy issue is whether these sets of law, which arose as a result of separate needs and separate problems, can or should be synthesized into a single regulatory scheme for the governance of criminal justice record information for noncriminal justice purposes.

The Task Force concluded that the most viable approach would be to regulate the use of criminal justice record information by applying FCRA-type protections on the end-user. The Task Force took the view that it makes little sense from a policy standpoint for privacy protections to apply to a background check if the employer obtains that information from a consumer reporting agency, but not in cases where the same em-

---

hand, in both *Cox Broadcasting* v. *Cohn*, 420 US 469 (1975) and *Florida Star* v. *BJF*, 109 S. Ct. 2603 (1981), the Supreme Court made clear that a court may restrict access to criminal history information maintained in court records on a case-by-case basis.

[470] *See, for example, Reporters Committee for Freedom of the Press* v. *Department of Justice*, 489 U.S. 749 (1989).

[471] *See, for example, New Bedford Standard-Times Publishing Co.* v. *Clerk of the Third District Court*, 387 N.E. 2d 110 (1979).

ployer obtains the same information, for the same purpose, directly from a court or repository rather than from a consumer reporting agency.

Some Task Force members also suggested that commercial vendors should not be restricted with respect to the information that they can collect and include in reports. Instead, restrictions, if any, should be placed on the ability of end-users to use such information for employment or other purposes. This approach also accommodates the purchase of criminal justice record information from courts and other sources on a bulk basis by commercial vendors. Under this approach, the commercial vendor does not have a particular use or purpose in mind. Instead, commercial vendors buy the information in bulk and maintain that information in their own data warehouse (frequently enhancing and enriching the information) for future requests and uses by end-users.[472]

Other Task Force members, while not opposed to the regulation of end-users, viewed regulatory controls on access to criminal justice record information held by the courts and government agencies as a viable approach for enhancing privacy and promoting other societal goals, such as reintegration of offenders into society. In short, if the data cannot be accessed, then it cannot be used. Regulation of specific data elements, such as the Social Security number, can both help protect individuals from identity theft and reduce the ability of commercial vendors to link personal data about individuals from multiple databases.

A few Task Force members took a different view, urging the imposition of restrictions on commercial vendors' access to criminal justice record information (particularly, preventing bulk sales of court and corrections data). They argue that this will protect privacy by preventing (or at least making it much more difficult) for commercial vendors to create comprehensive national background checking products to rival the State repository and FBI systems. This would reduce or effectively eliminate commercial vendors as an alternative to the repository system and, given the restricted or closed nature of those systems in most States, put the State legislatures firmly in control of who can access criminal history record information for which purposes.

Task Force members noted that constitutional and institutional concerns may limit the ability to consolidate the three bodies of law (court, repository, and vendor) into one coherent approach. As noted above, the law in each of these three areas evolved in response to different circumstances and concerns. The courts, for example, have a strong legal and cultural tradition of making their records publicly available (although not necessarily in bulk), the principal exception being specific instances where a judge determines that records should be sealed. Several Task Force members from public agencies emphasized that any effort to harmonize the law in this area should continue to distinguish between disclosures made by government instrumentalities and disclosures made by the private sector in light of these traditions and the public policy reasons for which courts and agencies make information available.

In addition, harmonization of these three bodies of law could have considerable financial implications, either in terms of new compliance costs or lost revenues. It was noted that many courts and State and local governments likely would resist a new Federal mandate unless the Federal law provided necessary funding. Other Task Force members noted that even if funding were not an issue, States likely would vigorously resist any attempt by Congress to mandate how State courts and criminal justice agencies may disseminate their criminal justice record information.[473]

[472] A 2002 decision by the Iowa Supreme Court under the Federal Drivers Privacy Protection Act (DPPA) balked at this approach to relevancy and prohibited a commercial vendor from buying motor vehicle records in bulk. The court interpreted the DPPA to require that a party purchasing motor vehicle and driver's license information from a State Department of Motor Vehicles must be able to meet one of the 14 specific uses under the DPPA and tie the particular record to that particular use. The case involved a commercial vendor that intended to buy driver's license information in bulk and disseminate it only to an end-user armed with at least one of the 14 permissible DPPA uses. Although the Court's decision was based on a technical reading of the DPPA, the underlying public policy interest focused on the fact that the vendor did not itself meet any of the relevancy criteria under the DPPA. The court, in other words, insisted that the commercial vendor, and not its end-user, meet the relevancy test. *See*, *LOCATE.PLUS.COM INC. d/b/a Worldwide Information, Inc.* v. *Iowa Department of Transportation,* 650 NW 2d 609 (2002).

[473] Several States, for example, vigorously opposed implementation of the Federal DPPA, 18 U.S.C. § 2721 et seq., which regulates State disclosure of motor vehicle records, unsuccessfully challenging the

With these difficulties in mind, the Task Force settled on the view that the most practicable way to harmonize the legal and privacy requirements would be to apply FCRA-type protection, regardless of the source of the criminal history data.

C. Are there relevancy considerations in the collection, use, and dissemination of criminal justice information?

Many believe that the Nation's information policy is inevitably migrating from a **scarcity model** (information was difficult and expensive to find; expensive and difficult to maintain, retrieve, and update; and, therefore, most if not all of the information collected was used) to a **relevancy model** (information is cheap and easy to find; cheap and easy to maintain, retrieve, and update; and, therefore, this wealth of data must be screened). Applying a relevancy model, the question becomes not what information can companies obtain, maintain, and use, but what information *should* companies obtain, maintain, and use?

The relevancy model for the collection, use, and disclosure of criminal justice record information remains in a very nascent stage. Information is increasingly readily available, but relevancy determinations are unclear. As a society, we know very little about whether, and under what circumstances, criminal justice record information (and different kinds of criminal justice record information) is relevant to various determinations involving employment, licensing, access to credit, insurance, housing, or other valued statuses or benefits.

As a result, the current default, especially in an increasingly dangerous and risk-averse society, is to allow all (or virtually all) criminal justice information to reach end-users and then permit end-users, based on their own needs, culture, and law, to sort out the relevancy of the information. Employers, for example, enjoy wide latitude in determining whether criminal justice record information about an individual should disqualify an individual from eligibility for a position, except in those cases where the law specifically prohibits consideration of certain information (such as arrest information in some States) or requires that individuals with certain criminal histories be barred from positions (as is the case for certain air transportation employees, for example). This latitude places the responsibility for risk management on the employer or other end-user, allowing them to weigh the potential costs (for example, liability, physical harm, lost training costs[474]) and benefits (for example, the individual's skills and talents) of hiring or otherwise interacting with an individual with a criminal record. This decentralized approach means that decisions may vary widely depending upon the risk management choices of the employer or other decisionmaker.

The question facing an employer or other end-user is whether an individual's particular interaction(s) with the criminal justice system (arrest, indictment, conviction, acquittal, etc.) should disqualify that individual for employment, either for any position or for a particular position. In addition to the nature and circumstances surrounding the interaction, *when* the offense occurred may also be a consideration. Timing can vary from a more or less contemporaneous interaction to events that occurred decades earlier.

The metrics for relevancy, of course, may vary, depending not only on the nature of the criminal justice record information involved, but also on its intended use. When hiring an individual to work in a daycare center, for example, it is likely to be considered

constitutionality of the statute. *Reno* v. *Condon,* 528 US 141 (2000).

[474]Economic loss as a result of employee theft or other malfeasance has been documented. *See, for example,* Hollinger Retail report, *supra* note 201. Research directly tying that loss to employees with criminal backgrounds is not as readily available, however. There is some anecdotal evidence, however. For example, ChoicePoint informed the Task Force that it "conducted a project with a well-known national retailer who rescreened their employees using ChoicePoint's National Criminal Record File and based on the results then studied the work history for those employed individuals that were found to have a previously unknown criminal record. This rescreen was run against employees that had passed the traditional limited county record check. The results of this rescreen discovered that the company hired 2,600 employees with criminal records, 1,100 of which had been terminated for workplace misconduct—including theft—within 6 months of being on the job. The average cost of the workplace misconduct was $1,000. The company determined that the cost to hire, train, and terminate an employee was $7,200. All told, this retailer estimates that the 1,100 employees with criminal records cost the retailer more than $9,000,000." ChoicePoint comments, *supra* note 50.

relevant that the individual has five arrests for child molestation, even if the individual has never been convicted of that crime. By contrast, the same information may not be so relevant if that same individual is being considered for a position as a bartender.

1. What is relevant?: The example of Eli Lilly

In the aftermath of the September 11 attacks, pharmaceutical manufacturer Eli Lilly revised its background-screening requirements, including those it required of more than 7,000 employees of its vendors, whose work assignments required access to Eli Lilly pharmaceutical manufacturing facilities. The policy changes required that vendors use a Lilly-picked vendor to conduct all background checks, using a standardized form.[475] Lilly originally proposed conducting credit and motor vehicle checks, as well as criminal background checks, but relented after union officials protested.[476]

According to union officials, when the results of the criminal checks were received, at least 100 workers were banned from Lilly facilities as a result of the checks.[477] This did not necessarily mean that the workers lost their jobs, since they actually worked for Lilly vendors, but many did lose their jobs because the vendors did not have any non-Lilly work for them to do. The company came under criticism when the nature of some of the offenses for which workers were banned came to light. One woman who worked as a pipe insulator, for example, allegedly was barred from the Lilly facilities as a result of a misdemeanor conviction for a $60 bounced check to a refrigerator-rental company, which she says occurred because she closed the account without realizing that the check had not yet cleared.[478] Another was arrested 6½ years before for "a misdemeanor battery charge that had since been dismissed."[479] A third "had been fined $250 and served 20 hours of community service 14½ years ago for misdemeanor marijuana possession."[480] Another had no criminal record at all, but was erroneously reported to have a record actually belonging to a relative with the same name.[481]

Lilly's actions were criticized. "I understand not employing a mad bomber, (but) it just doesn't seem right," was the reaction of one union official.[482] According to Indianapolis labor lawyer Bill Groth, "Lilly has really decided to crack down. A good point can be made that Lilly is overreaching… I don't know how the Indiana courts would look at this. It would be a difficult case."[483] Amid complaints, Lilly subsequently relented and allowed some contract workers it initially barred from its premises to return.[484]

[475]Associated Press, "Post-Sept. 11 background checks prompt layoffs at Lilly" (Feb. 2, 2002). Hereafter, AP Layoff article.

[476]Davis article, *supra* note 180.

[477]Ibid.

[478]Ibid.

[479]Ibid.

[480]Ibid.

[481]Ibid.

[482]AP Layoff article, *supra* note 475 (quoting Don Ireland, identified as a local union official).

[483]Ibid.

[484]Davis article, *supra* note 180.

2. Guidelines for relevancy

An area of particular interest to the Task Force was whether sufficient guidance is available to employers and other users of criminal justice record information. There were two broad areas where Task Force members thought guidance to end-users would be valuable: (1) understanding the meaning of the information provided, and (2) assistance in making relevancy determinations.

The Task Force considered developing such guidelines as part of its work, but could not reach consensus on this issue amid concerns that the composition of the Task Force was not appropriate for the preparation of such detailed guidance. In addition, some Task Force members expressed concern that even if the guidance produced was clearly designated as voluntary, many employers may feel compelled to comply because of the U.S. DOJ's sponsorship of the Task Force's work.

The Task Force noted that some guidance had been developed to assist end-users, such as employers, through the background screening process. For example:

- **Screening persons who work with vulnerable populations.** In 1998, the Office of Juvenile Justice and Delinquency Prevention (OJJDP), within the U.S. DOJ's Office of Justice Programs, published "Guidelines for the Screening of Persons Working with Children, the Elderly, and Individuals with Disabilities in Need of Support," which were developed in association with the American Bar Association's Center on Children and the

Law.[485] The Guidelines were developed to help meet a congressional mandate that the Attorney General "develop guidelines for the adoption of appropriate safeguards by care providers and by states for protecting children, the elderly, or individuals with disabilities from abuse."[486]

With respect to criminal background checks, the Guidelines:

> "…do not mandate criminal record checks for all care providers but do present advice on establishing a policy that provides an appropriate level of screening based upon specific situations… The first step presented in this decision model includes an assessment of 'triggers' that pertain to the setting in which the care is provided, the employee's or the volunteer's level of contact with the individual receiving care, and the vulnerability of the care receiver. The next step is weighing the availability of information, the costs of the screening, and the human resources needed to carry out the screening process. The third step is the analysis and selection of appropriate screening practices that would be used in addition to 'Basic Screening,' which includes reference checks, interviews, and a written application."[487]

- **Labor Policy Association Protocol.** In 2003, the Labor Policy Association (LPA) published the "LPA Background Check Protocol: Achieving the Appropriate Balance Between Workplace Security and Privacy." LPA is "a public policy advocacy organization representing senior human resource executives of more than 200 of the largest corporations doing business in the United States" and employing more than 19 million worldwide.[488] The Protocol was developed by the LPA Workplace Security Advisory Board, which is comprised of the top security officials of LPA member companies. According to LPA, the Protocol is:

  > "a model background check process that is designed to further the security interests of America's employers and the United States in several important respects. First, the Protocol serves to provide guidance to companies that may have little past experience with background check practices and may be grappling for the first time with the numerous complex issues inherent in conducting those checks. In addition, for companies that already have a background check process, the Protocol provides an opportunity to compare their processes against other companies, using the Protocol as a benchmark."[489]

  With respect to the criminal background component of a background check, the Protocol notes that the FCRA and State law regulate the types of criminal justice record information that can be reported and considered.[490] The Protocol characterizes the employer process for using criminal justice information to make an employment decision as follows:

  > Where not limited by state law, the employer may consider criminal convictions in making employment decisions. The mere presence of a criminal conviction should not necessarily render an individual ineligible for employment. In making such decisions, the employer should consider:
  >
  > - The circumstances and type of the crime;
  > - The length of time since the crime occurred;

[485]Office of Juvenile Justice and Delinquency Prevention, "Guidelines for the Screening of Persons Working With Children, the Elderly, and Individuals with Disabilities in Need of Support" (April 1998). Available at <http://ojjdp.ncjrs.org/pubs/guidelines/contents.html> (visited June 29, 2004).

[486]Ibid., at p. iii.

[487]Ibid.

[488]Labor Policy Association Workplace Security Advisory Board, "LPA Background Check Protocol: Achieving the Appropriate Balance Between Workplace Security and Privacy" (March 2003) at p. 3.

[489]Ibid., at p. 19.

[490]Ibid., at pp. 33-34.

- Whether the applicant has completed a rehabilitation program; and
- The applicant's employment record since the commission of the crime.

Determination of whether a crime is relevant to the job will generally be made on a case by case basis. For example, a conviction for driving while intoxicated may result in an adverse employment determination with regard to a delivery truck driver but not necessarily an accounting clerk. Similarly, a conviction for passing bad checks may disqualify the latter but not the former. For positions where integrity is particularly essential to the job, such as a corporate ethics officer, any conviction may be relevant.

However, there are certain crimes that will be relevant to the vast majority of jobs, including crimes of violence, such as murder, rape, robbery, and assault; and dishonesty-related crimes, such as theft, burglary, embezzlement, forgery, and fraud. Unrehabilitated drug-related crimes may also be considered, consistent with the Americans with Disabilities Act, for all positions. Multiple convictions, involving any combination of crimes, will also be considered as a factor in determining whether employment is appropriate.[491]

With respect to arrest records, the Protocol states:

> Generally, employers do not disqualify applicants on the basis of arrests where there was no conviction. Some employers may decide not to consider such arrests under any circumstances. Even where arrests are considered, the mere fact of an arrest typically should not, in and of itself, result in an adverse employment decision. That an applicant was arrested does not establish that the applicant actually committed the alleged crime. In addition, because the use of an arrest record in employment decisions may have a disparate impact upon certain protected classes, employers should be very careful about the use of such records in employment decisions.[492]

And with respect to ongoing matters:

> Where criminal proceedings are pending or where adjudication of a charge is deferred, the hiring process will often be suspended or terminated. In such instances, the applicant should be informed that he or she may reapply for a position with the employer after the proceedings are complete.[493]

- **Other sources.** The Task Force also noted that other sources of guidance exist, such as newspaper and magazine articles on the subject. In addition, in cases where a background check is conducted through a commercial vendor, the commercial vendor may provide the end-user with guidance as to what entries mean and whether an offense might be relevant to an employment or other decision.

3. Public policy issues

a. Who determines relevancy? Should public policy pivot on whether the criminal justice record information is conviction or arrest-only information?

A critical public policy question is whether employers and other end-users should be permitted to see all of this sensitive and heterogeneous information. Should they be permitted, indeed expected, to sort out all of this information based on their own determination of relevancy? Should society step in and determine relevancy either through legislation that prohibits the consideration of certain criminal justice information or by appointing a State agency or agent to evaluate the relevancy of criminal justice information on a case-by-case basis?

Recent legislation seeking to amend the National Child Protection Act (NCPA) takes the view that organizations providing care to the elderly, handicapped, and children should be permitted to

[491] Ibid., at p. 39.

[492] Ibid., at p. 40.

[493] Ibid., at p. 40.

see all of a criminal history record and determine for themselves, based on their own relevancy standards, whether any of that information is a disqualifier.[494] By contrast, current NCPA law permits only an authorized State agency to review a criminal history record in order to make a relevancy determination. Furthermore, NCPA law makes a sharp distinction between conviction information and nonconviction information.[495]

The Fair Credit Reporting Act also recognizes a sharp distinction between conviction information and arrest information. Under the FCRA, with certain exceptions, arrest information can be maintained in a consumer report only for 7 years from the date of the arrest. By contrast, the FCRA was amended in 1998 to permit the disclosure of conviction information in perpetuity and regardless of the date of the conviction.[496]

Many employers and landlords argue that they should be able to access as much information as possible to make the most informed choices.[497] Most commercial vendors agree, arguing that relevancy should not be an important consideration or litmus test in their effort to compile a complete criminal history record and communicate that record to an end-user. Both groups argue that an end-user should be able to see the entire record and then sort out the use of the record, based on the end-user's estimation of relevancy.

By contrast, some argue that if law and policy permits the entire record to be reviewed by an end-user, most end-users will have little choice, in an increasingly risk-averse society, but to opt not to hire (or not to provide other benefits or statuses to) a person with a criminal record. A proposed solution is the withholding of aged criminal justice information;[498] incidental or "minor" criminal justice record information; information about juveniles; and inconclusive (i.e., arrest) criminal justice record information.[499]

b. Is criminal justice record information relevant to terrorism-prevention efforts?

Questions have been raised about the relevance of the typical background check to screen out potential terrorists. Even representatives of some commercial vendors question whether a criminal background check, despite other benefits, can help prevent terrorism. As a spokesman for one commercial vendor put it: "Truth is, conventional methods for screening applicants would not, in most cases, screen out a potential terrorist."[500]

---

[494] *See*, H.R. 5556, The National Child Protection and Volunteers for Children Improvement Act of 2002, 107th Cong., 2nd Sess. (amending the NCPA at 42 U.S.C. § 5119c); *see also*, S. 22, 108th Congress, 1st Session (same).

[495] Ibid.

[496] Consumer Reporting Employment Clarification Act of 1998, Pub. L. No. 105-347 at § 5. The National Task Force on Privacy, Technology and Criminal Justice Information recommended that new criminal justice privacy law and policy "continue to give weight to the distinction between conviction information and non-conviction information." The Privacy Task Force noted that the distinction between conviction and nonconviction information has long been a "cornerstone" of criminal history privacy policy. The Privacy Task Force report further noted that nonconviction information carries with it a presumption of innocence; its dissemination frustrates efforts to reintegrate arrestees into society; and its dissemination may have a disproportionate impact upon minorities. Privacy Task Force report, *supra* 106, at p. 80.

[497] The Labor Policy Association, the National Apartment Association, and the National Multi Housing Coalition, for example, all support access to more criminal justice information either through reduction of State and Federal regulation of what information they can consider or through the increased availability of FBI background checks. See the following discussion of reintegration for additional information.

[498] Age of a criminal event, of course, depends upon the defining event from which age is measured (*for example,* arrest, conviction, release from incarceration, etc.). The FCRA places no restriction on the reporting of conviction information and restricts the reporting of arrest information, with certain exceptions, to 7 years from the date of entry of the arrest. 15 U.S.C. §§ 1681c(a)(2), (5). State law may impose more restrictive requirements. According to vendors, using the date of release as a standard could present difficulties for commercial vendors because data made available by corrections departments do not always include the release date.

[499] Restrictions in current law on the type of criminal history information that can be reported to a State repository or to the FBI reflect an implicit relevancy determination based on the content or sensitivity of various kinds of criminal history information. These kinds of restrictions may also, however, reflect the fact that, historically, it was expensive to compile, maintain, retrieve, and update information; thus, only the most important or serious information should be reported to a repository.

[500] Society for Human Resources Management, "Life Goes On: The Sept. 11 Attacks Were Over Within Hours, But the Effects Linger Even Today. This Is How Employers are Adapting," *HR* Magazine, Vol. 47: Issue 9 (Sept. 1, 2002) (quoting Steven James, Background Profiles Inc.).

According to another, "An identity check is probably a better preventative measure for terrorism than a criminal background check." [501] And a third: "We can help employers make sure the person they're hiring is who they represent themselves to be… What we can't tell is if they're a terrorist. There's no database for that."[502]

Without question, however, fear of terrorism has encouraged a heightened interest in knowing more about not only employees and prospective employees, but also customers (such as air travelers) and business partners. In some, albeit limited, cases, criminal justice record information may be directly relevant. An individual may be on the Most Wanted Terrorist List or may have previous terrorism-related arrests or convictions. Even if the typical criminal background check may not identify or predict a potential terrorist, does this matter? If a company decides to conduct background checks out of a terrorism-prevention motivation or simply to reassure itself or its customers, does it matter that the individual is subsequently disqualified not due to terrorism concerns, but because the report produced criminal justice record information the employer deems disqualifying?

[501]Curtis article, *supra* note 171 (quoting Gary Cornick, president of San Jose-based Peoplewise).

[502]Ibid. (quoting Renee Svec, spokeswoman for Florida-based HireCheck).

D. Do commercial vendor criminal justice information databases and the increased reliance on criminal background checks frustrate efforts to reintegrate offenders into society?

The current public policy regarding the employment, housing, and overall reintegration of offenders into society creates an anomaly. On the one hand, various laws and public policies encourage the reintegration of offenders into society. On the other hand, various laws and public policies encourage, permit, or require that criminal background checks be conducted for employment and housing purposes. This anomaly raises a number of public policy questions regarding how best to balance the need to reintegrate offenders into society with concerns that society has about public safety and recidivism.

1. Reintegration

The societal impact of the reintegration issue has grown in concert with the size of the prison population. That population has "nearly doubled since 1990 at the state level, increasing from 708,393 in 1990 to 1,277,127 at yearend 2002."[503] In 2000, "about 10% of Federal inmates and 49% of State inmates were in prison for a violent offense."[504] At current rates of incarceration, an estimated 1 out of every 20 persons (5.1%) will serve in prison during their lifetime.[505] In the case of certain males in certain minority groups, the estimates are considerably higher, suggesting that, "an estimated 28% of black males will enter State or Federal prison during their lifetime, compared to 16% of Hispanic males and 4.4% of white males."[506]

Most of these individuals eventually will be released back into the community. According to the Office of Justice Programs, "nearly 650,000 people are released from incarceration yearly and arrive on the doorsteps of communities nationwide."[507] This equates to about 54,166 people released each month, 12,500 released each week, and 1,786 each day. These individuals often need assistance reintegrating into society upon their release, as President Bush noted in his 2004 State of the Union Address:

> Tonight I ask you to consider another group of Americans in need of help. This year, some 600,000 inmates will be released from prison back into society. We know from long experience that if they can't find work, or a home, or help, they are much more likely to commit crime and

[503]Timothy Hughes and Doris James Wilson, *Reentry Trends in the United States,* section on "Growth in State prison and parole population" (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, April 2004) available at <www.ojp.usdoj.gov/bjs/reentry/reentry.htm> (visited June 29, 2004).

[504]Bureau of Justice Statistics, "Criminal Offenders Statistics" (Jan. 14, 2004) available at <www.ojp.usdoj.gov/bjs/crimoff.htm> (visited June 29, 2004).

[505]Ibid.

[506]Ibid.

[507]Office of Justice Programs, "Learn about Reentry," available at <www.ojp.usdoj.gov/reentry/learn.html> (visited June 29, 2004).

> return to prison. So tonight, I propose a four-year, $300 million prisoner re-entry initiative to expand job training and placement services, to provide transitional housing, and to help newly released prisoners get mentoring, including from faith-based groups. (Applause.) America is the land of second chance, and when the gates of the prison open, the path ahead should lead to a better life. (Applause.)[508]

As these individuals are released, they reenter local communities and usually need to find housing and/or employment. These reintegration efforts can be adversely impacted, however, by the fact that these individuals have been incarcerated. The future employment prospects of former inmates may be impacted by the stigma associated with imprisonment as well as "the erosion of human capital." As one researcher describes it: "[w]hile social stigma describes employers' perceptions of those with criminal records, the erosion of human capital refers to real deficiencies in the productivity of ex-inmates as a consequence of their imprisonment."[509]

This same researcher suggests that the stigma does have at least some impact on the reintegration of former offenders: "Employers were less likely to respond positively to ex-convicts than those who provided no information about past convictions. Recent survey data similarly suggest that employers would be more likely to hire welfare recipients or applicants with little work experience than ex-convicts."[510] At the same time, data suggest that "serving time in prison can diminish an individual's earnings, but not necessarily employment prospects."[511]

It does not appear, however, that all interactions with the criminal justice system result in the same adverse affect on offenders.[512] "If stigma attaching to criminal justice contact reduces earnings or employment, we might expect little difference in the effects of arrest, conviction, probation, or incarceration. From the employer's viewpoint, each intervention carries similar information about the trustworthiness of a prospective worker."[513] Some research, however, suggests differing economic impact as a result of arrest, conviction, probation, jail, and prison time.[514] "Prison is found to have an especially large and persistent negative effect on earnings, suggesting the impact of prison on the erosion of job skills."[515]

While the impact of criminal justice record information on the overall reintegration of ex-offenders may require additional research, it is clear that having a criminal record can exclude an ex-offender from certain jobs and housing activities. "At least six States bar ex-offenders from public employment. Federal laws bar many ex-prisoners from public housing and federally assisted housing programs. Some States place restrictions on fields of work ex-inmates can pursue, including law, real estate, medicine, nursing, physical therapy, and education."[516]

Negligent hiring doctrine, for example, also may act as an impediment to reintegration by discouraging employers from "taking a chance" on someone with a criminal record (particularly for serious offenses). Even if the employer tends to believe that the offender poses no threat, the employer may still elect to hire a

[508]President George W. Bush, "State of the Union Address" (Jan. 20, 2004) (transcript available at <www.whitehouse.gov>) (visited Jan. 21, 2004).

[509]Bruce Western, et al., *The Labor Market Consequences of Incarceration*, Working Paper #450 (Princeton University Industrial Relations Section, January 2001) at p. 4 (citations omitted). Originally prepared for the Urban Institute's Re-entry Roundtable, October 2000.

[510]Ibid., at p. 3.

[511]Ibid., at p. 21 (citations omitted).

[512]Current debate focuses on whether "the labor market experiences of ex-offenders [are] due to the effects of conviction or incarceration or are they due to characteristics of offenders that simultaneously place them at risk of arrest and low earnings or employment." In other words, whether incarceration is responsible for undermining the economic opportunities of ex-offenders or if "it may simply be officially earmarking severely disadvantaged men who would otherwise have poor job prospects, although without the dubious distinction of membership in a policy-relevant population." Ibid., at p. 2.

[513]Ibid., at p. 14 (citations omitted).

[514]Ibid., at p. 21. "[D]ata suggest that the earnings penalty of imprisonment ranges from 10 to 30 percent. By contrast, the evidence on employment and earnings penalties from arrest, conviction, and time in jail is uneven." Ibid.

[515]Ibid., at p. 14 (citations omitted).

[516]Geraldine Sealey, "No Second Chances? Ex-Prisoners Face Mounting Barriers to Re-entering Society," ABC News (Dec. 10, 2002) available at <http://abcnews.go.com/sections/us/daily-news/reentry_punishment021210.html> (visited April 9, 2004). Hereafter, Sealey newscast.

candidate without a criminal history to avoid potential liability.

Simple stigma also may impede an offender's reintegration. As one commercial vendor asserts in promoting a tenant-screening product, "Virtually all criminals live in rental housing. Do you really want them living in yours?"[517]

2. Recidivism

Undoubtedly, one of the reasons that reintegration and public safety goals conflict is the lack of confidence in society's ability to rehabilitate offenders. This lack of confidence is corroborated by recidivism. In June 2002, the Bureau of Justice Statistics released data from the largest recidivism study ever conducted in the United States, which tracked prisoners discharged in 15 States (representing two-thirds of all State prisoners released in 1994).[518] According to the study—

- 67% of former inmates released from State prisons in 1994 committed at least one serious new crime within the following 3 years. This rearrest rate was 5% higher than that among prisoners released during 1983.
- Most former convicts were rearrested shortly after getting out of prison: 30% within 6 months, 44% within 1 year, 59% within 2 years, and 67% by the end of 3 years.
- Within 3 years, 52% of the 272,111 released prisoners were back in prison either because of a new crime or because they had violated their parole conditions (for example, failed a drug test or missed a parole office appointment).
- These 272,111 inmates "had accumulated more than 4.1 million arrest charges prior to their current imprisonment and acquired an additional 744,000 arrest charges in the three years following their discharge in 1994."[519]
- The study also found that "post-prison recidivism was strongly related to arrest history. Among prisoners with one arrest prior to their release, 41 percent were rearrested. Of those with two prior arrests, 47 percent were rearrested. Of those with three earlier arrests, 55 percent were rearrested. Among those with more than 15 prior arrests, that is about 18 percent of all released prisoners, 82 percent were rearrested within the three-year period."

Robust recidivism and a lack of confidence in rehabilitation create a climate in which reintegration goals are viewed as too optimistic and too unrealistic to outweigh the public's very real interest in public safety.

3. Public policy options

a. Sealing and purging

The stigmatization that can be caused by criminal justice record information raises concerns that the availability of this information through government and commercial sources and increased reliance on criminal background checks may result in the creation of, "in essence, a subclass of citizens called former prisoners who are forever disadvantaged in their efforts to achieve reintegration … their sentence is never over."[520]

One means of promoting reintegration is to have that record sealed or expunged. "Nationwide, a growing number of convicted felons are seeking to erase any trace of past crimes as more employers perform background checks on job applicants—particularly since 9/11."[521] At present, laws in 40 States provide for the purging of nonconviction (that is, arrest-only) information and in 26 States for the purging, under some circumstances at least, of conviction information. Also, laws in 31 States provide for the sealing of nonconviction information and in 30 States for the sealing of

[517]First American Registry, "Products and Services: National Criminal Check," available at <www.residentscreening.com> (visited Jan. 21, 2004).

[518]Bureau of Justice Statistics, "Two-Thirds of Former State Prisoners Rearrested for Serious New Crimes" (June 2, 2002) available at <www.ojp.usdoj.gov/bjs/pub/press/rpr94pr.htm> (visited June 29, 2004).

[519]Another BJS study found that about 3 in 8 defendants in felony cases in State courts in the Nation's 75 largest counties in May 1998 had an active criminal justice status at the time of the current charged offense. Sixteen percent were on probation, 14% on pretrial release, and 5% were on parole. Bureau of Justice Statistics, "Criminal Case Processing Statistics" (Jan. 14, 2004) available at <www.ojp.usdoj.gov/bjs/cases.htm> (visited June 29, 2004).

[520]Sealey newscast, *supra* note 516 (quoting Jeremy Travis, senior fellow at the Urban Institute).

[521]Seth Stern, "Ex-felons see criminal records as a 'life sentence': Concern about fairness drives some states to consider laws that erase criminal records," *Christian Science Monitor* (Apr. 1, 2002) available at <www.csmonitor.com> (quoting Rob Karr of the Illinois Retail Merchants Association). Hereafter, Stern article.

conviction information.[522] (Purging, of course, means the destruction and/or redaction of information. Sealing customarily means that the information is no longer part of the official record; is stored separately, and is available for inspection only upon a court order).

Standards for purging and sealing vary substantially among the States, but typically pivot on the type of offense, the number of previous offenses, and whether the record subject has established a sufficiently long "clean record" period. Sealing and purging orders typically apply to criminal history information at the central State repository but not to original records of entry—for example, not to police blotter information at the station house and not to the court record (although judges can and do, in appropriate circumstances, order the sealing or even the destruction of court records). "About a dozen states do wipe out at least some felony convictions. Most require ex-convicts to stay out of trouble for a set number of years and will only expunge first offenses. Most, too, refuse to erase crimes such as murder, arson, and child molestation."[523]

The purging/sealing approach can restrict the flow of information from courts and government agencies, once the order is issued, but it does not guarantee that commercial vendors will have purged the information from their systems (though many may) or erase the event from media archives. Some vendors that obtain data in bulk seek to address the sealing and purging issues by periodically obtaining complete new data "dumps" from their sources (thereby limiting the information available to that which is currently available from the source agency). Not all vendors, however, necessarily undertake efforts to update their records to eliminate records that have been officially sealed or purged.

One vendor that does, National Background Data (NBD), attempts to address the issue by periodically obtaining new data dumps, as described above. However, expunged records may still be reported. If a disputed offense record has been expunged but is still in the public record information that NBD receives, the company deletes the expunged record upon receipt of a certified copy of the expungement documentation. If a prospective employer has already received the report, NBD also recommends that the consumer obtain a fingerprint-based background check from the State repository and helps the consumer locate the repository. Finally, NBD works with the agency that provided the expunged record to ensure that other expunged records are also purged from the data NBD receives.[524]

The obvious public policy question, is what, if anything, should be *required* to occur to a record held by a commercial vendor or the media when the underlying "official" repository record is purged or sealed. The Privacy Task Force report noted that in an information age, effectively "undoing" history may, as a practical matter, no longer be possible (or, perhaps, even desirable).[525]

b. Restricting end-user access and ability to use criminal justice record information

Another means of promoting reintegration is to legally regulate the use and/or disclosure of criminal justice record information for purposes of employment, housing, or other life activities deemed central to an offender's reintegration. With certain exceptions, for example, the FCRA prohibits consumer reporting agencies from reporting arrest information more than 7 years old (it does not, however, bar consumer report users from going directly to government agencies to get the information for themselves). In addition, State law regulates or prohibits the use of arrest and/or conviction information for certain purposes, such as employment. Of course, as previously noted, many State and Federal laws also mandate or encourage the conduct of criminal background checks for certain employment and housing opportunities.

c. Expanding end-user access and ability to use criminal justice record information

Both of the options discussed above effectively reduce the amount of criminal justice record information available to employers, landlords, and other interested parties. Those stakeholders, how-

[522]Privacy Task Force report, *supra* 106, at p. 76.

[523]Stern article, *supra* note 521.

[524]Robert W. Holloran, et al, "Special Issues Associated with Using Public Records in FCRA-Compliant Criminal History Background Checks," National Background Data Inc., presented to the 2nd Courtroom 21 Conference on Privacy and Public Access to Court Records, Williamsburg, Va., Nov. 2, 2002, at p. 23. Available at <www.courtaccess.org/legalwritings/nbd-specialissues2002.pdf> (visited June 28, 2004). Hereafter, Holloran Special Issues report.

[525]Ibid.

ever, typically want access to more, rather than less, criminal justice record information to make informed decisions that enhance safety and limit liability exposure. As one merchant association spokesman commented, "Retailers *do* hire people who've made mistakes…but we want to do it with our eyes open."[526]

This desire to enter into employment, housing, or other relationships with their "eyes open" is reflected in the legislative goals of employer and housing groups. The Labor Policy Association, for example, has called for Congress to amend the FCRA to, among other things: (1) preempt State laws limiting inquiries into arrest and conviction records; (2) remove the FCRA's 7-year limit on certain information (which the group believes to be arbitrary); and (3) expand the ability of employers to conduct background checks through the FBI.[527] With respect to the latter point, the National Apartment Association and the National Multi Housing Council also have made obtaining a broader ability to conduct background checks through the FBI a legislative priority.[528]

E. Should commercial vendors be permitted/ encouraged/ required to use a biometric when identifying individuals who are subject to criminal history record checks and when matching criminal history record information with a particular individual?

The Task Force took note that commercial vendors have made impressive strides in using name and other information to make reliable identifications. Nonetheless, the Task Force urged the commercial industry to more aggressively incorporate biometrics, and primarily fingerprints, into their identification processes.

With rare exceptions, State criminal history record repositories and the FBI create criminal history records only when the demographic information associated with the record (such as name, address, and other explicit identifiers) is supported by a fingerprint.[529] This ensures that these repositories will not maintain duplicate records about the same individual (who, perhaps, is using an alias or a slightly different name). Moreover, the association of a biometric—a fingerprint—with the record means that when the record is retrieved or when additional information is added to the record, there is an assurance that the right record has been retrieved or that the right updating or amending information has been appended to the right file. All of this is not merely a matter of good practice or even uniform practice but is mandated by State law, as well as applicable Federal law.[530]

Commercial vendors, on the other hand, customarily have relied upon name-plus-identifier checks. This reliance has been driven in part by necessity (since commercial vendors customarily have not had access to fingerprint-based checks), as well as the fact that name-plus-identifier checks have customarily been far less expensive than fingerprint-based checks and could be processed far more quickly. As fingerprinting technologies improve, however, the cost and time necessary to conduct fingerprint-based checks decline. The Task Force believes that the time has arrived when any cost or timeliness benefits derived from name-plus-identifier checks are outweighed by potential accuracy problems.

1. Benefits of fingerprint-supported checks

The benefits of associating fingerprints with criminal history records are well documented. A fingerprint-based check virtually eliminates the occurrence of a "false positive." False positives are easy to come by. It is estimated, for example, that there are 23,000 individuals with the name "Michael Smith" in the United States. It is also estimated that approximately 3,000 of these Michael Smiths move every year (thus, rendering address informa-

[526]Stern article, *supra* note 521.

[527]LPA FCRA memoranda, *supra* note 411, at p. 6.

[528]NAA/NMHC Joint Legislative Program, *supra* note 207.

[529]2001 Use and Management report, *supra* note 236, at p. 28.

[530]*See, for example,* The National Crime Prevention and Privacy Compact Act, 42 U.S.C.A. §14611 et seq.

tion unreliable).[531] A report of the National Task Force on Interstate Identification Index Name Check Efficacy found, in a sample of more than 82,000 individuals, that 4,562 were inaccurately indicated by name-plus-identifier checks to have criminal records. This represents approximately 5.5% of the sample.[532]

The occurrence of false negatives arising from name-plus-identifier checks presents even more serious public policy questions. When a name-plus-identifier check is used, a false negative can occur if the individual uses an alias; if an individual materially misstates his name or other identification; if the identifying information is mistranscribed; or if a simple search error is made.[533] The Name Check report found that, out of more than 82,000 individuals in the sample, 10,673 had fingerprint-verified criminal history records but of these, 1,252 were indicated by name-plus-identifier checks *not* to have a criminal history record. This means that about 11.7 percent of all those applicants with criminal history records were "beneficiaries" of a false negative.[534]

From a public policy standpoint, obtaining a fingerprint before conducting a criminal background check has another important benefit. The act of obtaining the fingerprint serves as more or less dramatic notice to the individual that a check will be conducted. Furthermore, because, for all practical purposes, it is not possible to obtain a fingerprint without the record subject's cooperation, the fingerprint requirement also can act as an informal or *de facto* form of consent.

2. Benefits of name-plus-identifier checks

Law, tradition, and perhaps even common sense, all suggest that criminal justice records that are supported by fingerprints and that are retrieved, updated, and amended based on fingerprints are more reliable than criminal justice records that are retrieved, updated, and amended based on name. The Task Force notes, however, that experience does not quite bear this out.

Commercial information vendors have seldom, if ever, had access to fingerprints or, for that matter, access to fingerprint-supported criminal history repositories. As a consequence, they have had little choice but to use name and other identifiers.

In the case of false positives, relevant laws (the Federal Fair Credit Reporting Act and similar State laws in a majority of the States) require that an individual whose consumer report is used as a basis for denying employment will obtain access to that report. Even when the FCRA does not apply, there are many other instances when an individual who is falsely and incorrectly identified as having a criminal record obtains notice of the reported record (and, indeed, is often asked for an explanation of the reported record).

Of course, when confronted with a resourceful and determined offender who is willing to use an alias and able to back up the alias with fraudulent identification, a name-plus-identifier check can (and, in fact, usually will) produce a false negative. This shortcoming may be mitigated, however, to the extent that the population that is the subject of background checks for noncriminal justice purposes is less apt to use aliases and to present fraudulent identification than the population that is arrested. Nonetheless, the risk of false negatives arising from name-plus-identifier checks cannot be dismissed and, indeed, was found to be significant by the National Task Force on Interstate Identification Index Name Check Efficacy.

Large and sophisticated commercial information vendors, however, use skip trace reports and other information resources to identify individuals who seem to have concocted fictitious aliases. On the other hand, individuals who fraudulently adopt a name and identification of an existing individual (and, presumably, one who operates without the benefit of a criminal justice record) present a far more serious challenge.

---

[531] Testimony of LexisNexis before the U.S. Senate Commerce Committee, May 23, 2002.

[532] *Interstate Identification Name Check Efficacy: Report of the National Task Force to the U.S. Attorney General,* NCJ 179358 (Sacramento: SEARCH Group, Inc., July 1999) at p. 3. Available at <www.ojp.usdoj.gov/bjs/pub/pdf/iiince.pdf> (visited June 29, 2004). Hereafter, Name Check report.

[533] False negatives can also result from other factors. False negatives can occur, for example, if information that would produce a positive result exists in databases that have not been checked as part of the search. False negatives may also occur in cases where an offense exists, but it has not been incorporated into a database because it does not meet an agency's criteria for inclusion (for example, it is not fingerprint-supported, it is a misdemeanor offense and the database checked includes only felonies, etc.).

[534] Name Check report, *supra* note 532 at pp. 6–7.

Nevertheless, some commercial vendors report low false negative rates. According to ChoicePoint, for example, "[i]nternal statistical reviews show that approximately one-half of one percent of the criminal record histories that are disputed results in ChoicePoint having to amend the report because of a false negative."[535] It is unclear, however, whether other commercial vendors have a comparable false negative rate.

There are other reasons why commercial vendors (and their customers) have been comfortable using name-plus-identifier checks. First, not all criminal justice record information is fingerprint-supported (for example, records of low-level misdemeanors or certain driving offenses are often not fingerprint-supported and therefore would likely not be produced as a result of fingerprint-based checks). Second, name-plus-identifier checks customarily cost far less than a fingerprint-based check. Third, name-plus-identifier checks have, at least until quite recently, taken far less time to complete than a fingerprint check. Fourth, in the noncriminal justice arena, there has traditionally been a "stigma" associated with being required to provide a fingerprint. This is especially true when individuals have been asked to go to the local police station to have their prints "rolled."

Finally, for commercial vendors there has been an element of "making a virtue out of a necessity." Commercial vendors seldom have access to fingerprints. Even if they were to obtain a fingerprint, commercial vendors routinely by law, regulation, or practice are denied access to repositories whose criminal history records are organized and supported by fingerprints (such as State central criminal history record repositories).

3. Increasing use of biometrics in the private sector

Today, the environment with respect to the availability and use of biometrics, including fingerprints, is changing rapidly. Biometrics are becoming commonplace. They are losing whatever stigma was associated with "being fingerprinted." Biometrics, for example, can be found on driver's licenses in many States (customarily, a thumbprint); are used for identification verification on checks by some banks and convenience stores; and are used in many other government and privately used identification systems. Further, more and more individuals are required to use a biometric as a password surrogate to log onto their computer or gain access to secure areas of their workplace or in other venues.[536]

Public opinion polls also indicate that the public is becoming more comfortable with biometrics. In a 2002 public opinion survey, a majority of respondents indicated that they would be comfortable with providing a fingerprint—particularly where the print is not rolled but, instead, is obtained by a process that is similar to putting an individual's thumb or fingers on a photographic plate.[537]

Even if commercial vendors continue to be prohibited from submitting fingerprints to repositories, if commercial vendors could use the fingerprinting process to positively verify the identity of an individual, then the vendor could submit the correct name with confidence that the vendor is not facing an alias and/or counterfeit identification. Indeed, law enforcement agencies increasingly are using a version of this approach in the criminal justice context by submitting a name-plus-identifier check (for speed and economy) and later verifying the results with a fingerprint, at least in those cases where there is a question of identity or authenticity.

Over the next 10 years, it seems increasingly likely that virtually all courts and criminal justice agencies will support at least new entries to their record system with a biometric. (Indeed, 20 years ago, almost no court records were automated. Today, court records are increasingly automated—suggesting the speed with which courts can make and have made progress in their information management capabilities.)[538]

Public policy in the privacy area is frequently challenged and, indeed, complicated by advances in technology. In this instance, however, technology and, specifically, the proliferation of biometric technologies, also may work to solve or mitigate problems associated with the collection, management, and retrieval of criminal justice

[535]ChoicePoint comments, *supra* note 50.

[536]Morris, "Tracking Work Done by Touch, Not Punch," *New York Times* (Jan. 17, 2002).

[537]Opinion Research Corp., "Public Attitudes Toward Identification Technologies, Crime Prevention and Privacy," (Aug. 15, 2002).

[538]Polansky, *Computer Technology in the Courts* (Westport, Ct.: Greenwood Press, 1980).

information by commercial vendors.

In anticipation of this progress, the National Task Force on Privacy, Technology and Criminal Justice Information recommended that, "criminal history record information, whether held by the courts, by law enforcement, or by commercial compilers and resellers, should, subject to appropriate safeguards, be supported by and accessible by fingerprints to the extent legally permissible and to the extent that technology, cost and the availability of fingerprints to both database managers and users, make this practicable."[539] The Commentary to that recommendation notes that changes in technology, particularly livescan fingerprinting, may soon make fingerprinting, "just as quick, convenient and inexpensive as [name-plus-identifier] checks."[540]

The Task Force agrees. The Task Force concluded that commercial vendors should be "encouraged" to use biometrics, and specifically fingerprints, to the fullest extent possible.

On the other hand, the use of biometrics by commercial vendors will, inevitably, raise privacy concerns, including whether biometrics and biometric-supported databases will be consensual, and whether these technologies could encourage surveillance activities or the development of a national identification system. The Task Force urged that appropriate attention be given to these issues.

4. Efforts to exclude certain descriptors from public records

In recent years, Congress, State legislatures, the courts, and government agencies have been grappling with the privacy issues raised by the loss of the *de facto* privacy standards that existed when all government records were part of manual systems that were once much more difficult to access (though still publicly available) than they are in the automated Internet age. The growth of identity theft as a crime also has prompted significant policy concerns.

One approach to addressing identity theft concerns and increasing privacy protections is to restrict access to, or prohibit the inclusion of, information in public records that is deemed to be too private (such as certain financial information) or a potential facilitator of identity theft. The Social Security number, given its extensive use by the government and private sector for record organization purposes, as an account number and a means of verifying identity, falls into the latter category. Also in the latter category are other identifiers, such as date of birth and mother's maiden name, given that this information is also frequently requested by institutions as a means of verifying the identity of the individual for purpose of providing account information over the telephone, for example. Many policymakers and privacy advocates believe that it essential to reduce the public availability of Social Security numbers to protect personal privacy, prevent identity theft, and weaken the Social Security number as the *de facto* national identification number.

Removal of the Social Security number and other identifiers from criminal justice records could, however, undermine the accuracy of name-plus-identifier-based background checks. As discussed above, name alone is not a sufficient basis for confidently returning the results of a criminal background check; additional descriptors are essential. Address can be used, but given the transient nature of the population, address is of only limited utility. Similarly, physical description can vary over time; besides which, it is not included in many criminal justice records. As a result, the Social Security number and date of birth are very important to the industry's efforts to provide accurate name-plus descriptor checks.

The Task Force notes that removal of these identifiers from public records could increase the potential for false positives or effectively limit the ability of commercial vendors to provide criminal background checks on a name-plus-identifier basis because the reports produced would not be sufficiently reliable. Removal of these identifiers may also increase the cost of the commercial vendors' products. An increase in false positives is potentially damaging to the individuals involved and also increases costs. Loss of the ability to conduct reliable name-plus-identifier checks would be likely to increase the demands on Congress and the State legislatures for access to fingerprint-based checks through the FBI and the State repository system.

[539]Privacy Task Force report, *supra* 106, at p. 75.

[540]Ibid.

F. Do commercial vendor criminal justice record checks suffer from completeness, accuracy, or timeliness problems and, if so, what types of public policy "fixes" should be employed?

1. Data quality challenges

As noted earlier, the primary sources of criminal justice record information for commercial vendors have, by far, been the courts. Court records, however, are comprehensive (if even then) only with respect to events that occurred in that particular court. This means, for example, that lower court records do not always include dispositions. Furthermore, events that took place in other courts, whether arising from the same or separate or subsequent events, are found only in the records of these other courts.

This dispersion of records presents a significant challenge to commercial vendors relying upon court records as their only, or at least primary, source of criminal justice record information. Vendors use various types of screens and sources (employment checks, SSN traces, motor vehicle records, records of prior addresses, etc.) to identify relevant jurisdictions and, thus, relevant courts whose databases should be searched. Such an approach to defining the scope of a criminal background check conducted by a commercial vendor customarily has been viewed as appropriate by the marketplace. The marketplace recognized that conducted a national search of criminal records on the chance that the individual may have committed a crime while passing through a distant jurisdiction was impractical.

With the recent growth of commercial "nationwide" criminal justice information databases, however, at least one vendor, National Background Data, has suggested that the customary local check is no longer sufficient, arguing that given technological advances, "Failure to check counties and states beyond the applicants' current and recent residences can no longer be justified on the basis of cost and time required to check other areas."[541] At the same time, however, commercial vendors still see a role for local agency checks. As Rapsheets.com notes, "Though much of the data provided by Rapsheets.com is the most complete and up to date information available instantly on the Internet, the service provided here does not always substitute for an in-person courthouse search of criminal records."[542] Many vendors also take care to note the sources of the information in their databases, putting users on notice that the database is not necessarily comprehensive and allowing the end-user to identify gaps in the vendor's coverage that may be relevant to the end-user's decision whether or not to use the database.

In addition, it is always possible for a commercially conducted, court-based, criminal check to miss an available disposition or even to miss altogether a particular prosecution, although as previously noted, commercial vendors "salt" their requests for court records as a quality control measure. Where an individual is detained or even arrested but no charges are brought and the individual is never indicted or arraigned, it is more likely that a commercial vendor check will not uncover this information.[543]

Other "data quality" problems confront commercial vendors. There is, of course, the problem, discussed earlier, that can arise when a name-plus-identifier check is incorrect and the wrong criminal justice record information is matched with the wrong individual. Furthermore, when criminal justice record information is bought in bulk, as opposed to obtained from a repository or a court in response to a customized, one-off search, the information obtained in bulk grows stale from the date of its acquisition and must be updated in a continual and systematic way in order to capture dispositions or other events.[544]

---

[541] Holloran Special Issues report, *supra* note 524, at p. 11.

[542] Rapsheets.com, "A History of Delivering Public Records," available at <www.rapsheets.com/business/info/history.aspx> (visited June 28, 2004).

[543] Some commercial vendors have policies against reporting arrest information where subsequent adjudication never occurred. For example, "ChoicePoint's Employment Service Center's current policy for reporting criminal record information is to report only criminal record information where some type of adjudication has occurred or the case is currently pending an upcoming court appearance." ChoicePoint comments, *supra* note 50.

[544] This is not to say that searches done by end-users directly with the State central repository or the FBI (when permitted) or directly with the courts are necessarily free of data quality problems. State central repositories customarily do not maintain records of "non-serious" events—defined

2. Fair Credit Reporting Act protections

When commercial vendors provide criminal justice records under the Federal Fair Credit Reporting Act and under State FCRA laws, protections exist that promote the accuracy, completeness, and timeliness of the records. Section 607 of the FCRA, for example, requires consumer reporting agencies to have in place "reasonable procedures" to ensure maximum possible accuracy.

Furthermore, where public record information (defined to include criminal justice record information obtained from repositories or courts) is obtained by a consumer reporting agency for an employment purpose, and where that criminal justice record is likely to have an adverse effect upon a consumer's ability to obtain employment (by definition, a criminal justice record), then the consumer reporting agency must, at the time that the agency provides the criminal justice record to the end-user, notify the consumer that this information is being reported and indicate the name and address to whom the information is being reported or maintain "strict procedures" designed to ensure that the information is complete and up to date. The FCRA goes on to say that, "items of public record relating to arrests, indictments, convictions…shall be considered up to date if the current public record status of the item at the time of the report is reported."[545]

In addition, under the FCRA a consumer can request access to the report and can seek to amend or correct inaccurate information in the report. As a practical matter, any time a commercial vendor subject to the FCRA reports criminal justice information to an employer for an employment purpose, the consumer must be given notice and will have an opportunity to review and correct the criminal justice record information in question. This is an important protection that enhances the likelihood of accuracy and completeness in the criminal justice information ultimately used to make an employment determination.

The FCRA does not apply in instances where end-users go directly to court, a repository, or other agency to obtain the records themselves. In addition, the FCRA applies only to commercial vendors with criminal justice record products that are used or expected to be used for FCRA-permissible purposes. Even where the FCRA's protections do apply, notice to the consumer relieves a consumer reporting agency of certain accuracy obligations. Some argue that the FCRA inherently recognizes that despite a vendor's best efforts, errors will occur and builds in notification procedures and reinvestigation requirements to compensate for this. Others argue, however, that these safeguards should not be used as an excuse by commercial vendors to rationalize inaccurate reporting.

As a result, the FCRA does not necessarily settle the accuracy and completeness issue. The extent to which commercial vendors should be permitted to make honest mistakes or experiment with new uses of information or technology, even if some inaccuracy may result, is a question for both policymakers and the marketplace. Accuracy is clearly a desirable goal, but too stringent an accuracy requirement (and accompanying liability) could discourage private sector participation in the conduct of criminal background checks. This, in turn, could indirectly work against the public policy interests served by the conduct of criminal background checks.

---

variously in the States, but usually comprising at least some misdemeanors. Further, although State central repositories exist for the purpose of compiling a comprehensive record of all criminal events relating to an individual that have occurred in that State, research indicates that arrests are sometimes (and, in some States, frequently) not reported to the repository. Moreover, by definition, a State repository maintains a record of only those offenses that have occurred in that State. While a State repository can initiate a national search to obtain criminal history records about an individual from other States, the fact remains that an in-state-only search is just that.

The FBI's criminal history database has its own data quality problems. By its own admission, the FBI obtains available dispositions for only approximately 50% of the arrest records held by the FBI. Furthermore, of course, many arrests are not even reported to the FBI, particularly arrests for nonreportable (minor) offenses. Finally, both the State repositories and the FBI are far more apt to have accurate, complete, and timely information with respect to events that have occurred during the last 10, and particularly, the last 5, years. Older criminal history record information, particularly where the individual has established a clean record period that includes the most recent 10 years, is apt to be incomplete, inaccurate or missing altogether.

It also must be emphasized that when end-users, such as employers, attempt to go directly to the courts for criminal history record checks rather than using a commercial vendor, most experts believe that the risk of obtaining inaccurate or incomplete information balloons.

[545] 15 U.S.C. § 1681k.

It was the sense of the Task Force that, on the whole, there is not a substantial reliability issue with respect to commercial vendors because commercial vendors have a strong business interest in trying to produce reliable, accurate, and complete products.

G. When commercial vendors combine criminal justice record information with other personal data to create a "profile," what are the public safety and risk management benefits, and what are the privacy threats? Does there need to be a public policy focus on this issue?

1. Reasons for profiling

There is little question that combining various types of personal information creates an information dividend for end-users that are making hiring decisions; decisions about accepting volunteers for youth groups and sports organizations; licensing decisions; and other decisions about benefits, statuses, and entitlements.

In making an employment decision, for example, criminal justice record information is often deemed to be relevant by employers. Of course, other kinds of personal information also are relevant to an employment determination, such as educational records and background; prior employment; motor vehicle and drivers' records (especially if the position involves driving for the prospective employer); credit history (particularly if the position involves access to or responsibility for corporate funds); medical history if the position requires a particular fitness level or physical activity (and subject to the strictures of the Americans with Disabilities Act); and even prior addresses (how close does the applicant live to the job and have there been problems with landlords, etc.). Furthermore, enhanced demographic information has become increasingly important to ensure that the person applying for the job is, in fact, who he says he is. A 1998 study by the Society for Human Resource Management, for example, found that "over half of the employers that check references on applicants discover some kind of false information and 45 percent of them found applicants lied about criminal records."[546] Combine this with the pressure on employers to hire the right person for the right job, and the burgeoning employer appetite for comprehensive background information is easily explained.[547]

Employers, to continue our example, customarily look to three sources for information about applicants. First, employers obtain a great deal of information from the applicants themselves. Second, employers can look to consumer reporting agencies to provide all or most of the personal information that an employer may deem relevant together with criminal justice record information. Third, employers can "shop" and obtain different pieces of relevant background information, either directly from various sources (such as going to schools and colleges to check an individual's educational background) or from various vendors. In this model, it is the employer—not the vendor—who puts together a comprehensive background assembled from a variety of sources.

2. Profiling and privacy risks

From a record subject's/applicant's privacy standpoint, it's not at all clear that it makes a difference whether the employer obtains a turnkey, comprehensive information profile from one vendor or whether the employer uses its in-house human resources staff to assemble the same profile from a variety of sources. Either way, the employer in our example ends up with a considerable amount of information about the applicant.

In point of fact, however, because the FCRA and its State law equivalents provide significant privacy protections if the applicant's information is compiled and communicated by a consumer reporting agency, the record subject/applicant enjoys the most protection if an employer buys a turnkey product from a consumer reporting agency. A privacy downside in the information vendor model, however, is that now two parties have access to, and perhaps maintain, this report: the employer and the consumer reporting agency (but, of course, the report remains subject to the FCRA).

---

[546] Labor Policy Association, "Reauthorization of the Fair Credit Reporting Act," Memoranda (March 8, 2003) at p. 7.

[547] Making an appropriate hiring decision is important for employers for cost reasons; for post-September 11 concerns, and for concerns arising from the negligent hiring doctrine. *See,* Robert Hunter, "Past as Prologue: Assessing Job Candidates" (March 2002) available at <www.securitymanagement.com> (visited Jan. 21, 2004).

The Privacy Task Force report focused on the privacy risks posed by criminal justice record databases that are "enriched" by other types of personal information. The Privacy Task Force recommended that, "criminal justice record information law and policy should restrict the amalgamation of criminal justice record information in databases with other types of personal information except where necessary to satisfy public policy objectives."[548] The Privacy Task Force noted, however, that there are instances where the amalgamation of criminal justice information with other types of personally identifiable information is necessary to further public safety.

The Privacy Task Force took the position that official criminal record databases maintained in State central repositories and the courts should not be "tainted" with non-criminal justice information. At the same time, the Privacy Task Force recognized that commercial vendors that "gather both CHRI [criminal history record information] and other types of personal information from disparate sources as part of an investigation, consumer report background check or similar inquiry" are beneficial and should "remain unchanged."[549]

The Commercial Sale of Criminal Justice Record Information Task Force does not express a view on whether policymakers should create barriers to the creation of amalgamated profiles. Some members of the Task Force argued that the amalgamation of criminal justice data and other types of data into a comprehensive profile on the individual should be resisted because, once a comprehensive database has been built, it cannot (or will not) be redivided into its component parts. As a result, these amalgamated databases will only continue to grow both in terms of data content and in terms of uses.

Other Task Force members questioned whether such a regulatory approach would be viable. Some Task Force members argued that technological advances in search software capabilities have made the idea that privacy can be protected by preventing the combination of data from multiple databases into one database an outdated concept because there may be little difference between going to one database for the information and doing a Google search and pulling the data from two separate databases.

Some members of the Task Force representing commercial vendors noted that their systems currently rely upon multiple databases (organized by information source or data type), not one master database; some or all of these databases are searched in the course of responding to an end-user's request, depending upon the scope of the search the end-user requested. Other Task Force members emphasized that these matters cannot (and should not) be addressed in the abstract. Prohibiting the use of a particular type of technology is not a viable approach. Instead, policymakers should identify specific undesirable acts and prohibit them.

[548]Privacy Task Force report, *supra* 106, at p. 78.

[549]Ibid., at p. 79.

Conclusion

In September 2004, the House Republican leadership introduced H.R. 10, the "9/11 Recommendations Implementation Act." Buried in that 609-page bill was a provision that gave private employers, with State authorization, direct access to the FBI's Integrated Automated Fingerprint Identification System (IAFIS) for criminal history record employment background checks. While this provision did not become law, its inclusion reflected growing congressional concern about not only the number of requests for statutory authorization for criminal history employment background checks, and not only the variety of types of jobs and other positions that would be subject to these checks, but also the utter lack of a consistent national approach to backgrounding.

Sometimes, State and Federal bills call for fingerprint-based checks, and sometimes not. Sometimes, State and Federal bills specify that the check should go through the State repository or through the FBI, and sometimes not. Sometimes, State and Federal bills specify the type of criminal history record to be obtained (conviction versus nonconviction, etc.), and sometimes not. And sometimes, State and Federal bills prescribe various privacy protections, and sometimes not.

As our Nation—at least on a *de facto* basis—moves rapidly toward universal backgrounding, it is certainly understandable that members of Congress and other policymakers are alarmed that no blueprint is in place for prescribing and regulating these checks. The Nation's security, as well as on-the-job efficiency, and certainly civil liberties and privacy interests, all demand the development of a blueprint. One part of that blueprint, undoubtedly, must lay out the role of commercial background screening companies.

This report, and the work of the Commercial Sale of Criminal Justice Record Information Task Force, represents an important and first-ever effort to lay the groundwork for drafting that blueprint, especially as it relates to the role of commercial background screening companies.

Appendix: Task Force members

Chair

Professor Kent Markus
Capital University Law School
Ohio

Members

Lana Adams
Law Enforcement Liaison
Program Services
Federal Investigations Service
U.S. Office of Personnel Management

Melvin Carraway
Superintendent
Indiana State Police

Francis D'Addario
Vice President
Partner and Asset Protection
Starbucks Coffee Company

John Ford
Chief Privacy Officer
Equifax, Inc.

Bud Gaylord
Director
Case Analysis and Support Division
National Center for Missing & Exploited Children

Lt. Col. Jeffrey Harmon
Deputy Chief
Maine State Police

Juanita Hicks
Clerk of Superior Court
Fulton County (Georgia) Superior Court

Robert Holloran
Chief Executive Officer
National Background Data, LLC

Robert Kamerschen
Vice President
Law and Public Policy
ChoicePoint, Inc.

Marc Krass
Associate General Counsel
The Procter & Gamble Company

Carlos Lacambra
Vice President
A-Check America

Lewis Maltby
President
National Workrights Institute

Garry Mathiason
Senior Shareholder
Littler Mendelson

Stuart Pratt
Executive Vice President
Governmental Relations
Associated Credit Bureaus, Inc.

James Shea
Assistant Director
Office of Systems
New York State Division of Criminal Justice Services

Solveig Singleton
Senior Policy Analyst
Competitive Enterprise Institute

Tim Spainhour
Legal Compliance Leader
Acxiom Corporation

Donna Uzzell
Director
Criminal Justice Information Services
Florida Department of Law Enforcement

Richard Velde
Attorney-Advisor

Kush Wadhwa
Senior Consultant
International Biometric Group

David Walchak
Deputy Assistant Director
Communications/Technology Branch
Federal Bureau of Investigation

U.S. Department of Justice

Carol G. Kaplan
Chief
National Criminal History Improvement Programs
Bureau of Justice Statistics

SEARCH, The National Consortium for Justice Information and Statistics

Sheila J. Barton
Deputy Executive Director

Robert R. Belair
Oldaker, Biden & Belair
General Counsel

Kevin Coy
Oldaker, Biden & Belair
Associate

Owen M. Greenspan
Justice Information Services Specialist

Eric C. Johnson
Policy Research Analyst

Task Force members and staff are listed with their titles and agency affiliations at the time of their participation in Task Force deliberations and the development of this report.